ADR-037 — Bilko Native Mobile + Entra External ID Auth

ADR-037 — Bilko Native Mobile Companion and Entra External ID Auth

> **Status:** Accepted for mobile direction / Phase 0 backend work required
> **Date:** 2026-06-04
> **Scope:** Bilko customer-facing mobile companion app for iPhone and Samsung/Android

Context

Bilko has existing web-first documentation that previously assumed a PWA path for MVP mobile support. Dedicated mobile docs later proposed React Native + Expo, but the architecture doc still marked the decision as recommended/not final and the implementation spec was marked ready for dispatch despite unresolved backend/auth blockers.

The product direction is now native mobile delivery for iPhone and Samsung/Android, not PWA as the primary mobile companion path.

Current backend auth evidence reviewed before this ADR:

- `apps/api/src/main/kotlin/no/alai/bilko/routes/AuthRoutes.kt` uses httpOnly refresh-cookie behavior for web.
- `apps/web/lib/api.ts` uses browser-oriented `credentials: include` refresh handling.
- React Native must not depend on browser httpOnly cookie refresh semantics.

Decision

1. Bilko Mobile Companion will use **React Native + Expo** for iOS and Android.
2. The previous **PWA-for-MVP** assumption is superseded for the mobile companion workstream. Responsive/PWA web may still exist as web capability.
3. Customer login for mobile should use **Microsoft Entra External ID** with **OIDC Authorization Code + PKCE**.
4. Bilko backend must provide an auth bridge that validates Entra identity, maps/creates Bilko user/org/role context, and issues/refreshes Bilko API/session tokens without relying on browser-only cookies.
5. Phase 1 mobile build is not dispatch-ready until Phase 0 auth/backend prerequisites are closed.

Phase 0 Backend Prerequisites

- Entra External ID tenant/app registration for Bilko customer login.
- Redirect URI configuration for Expo development, staging, and production builds.
- Backend token validation against Entra issuer/audience/JWKS.
- Bilko user, organization, and role mapping/provisioning.
- Mobile-safe session/API token issuance and refresh path.
- Logout/revocation behavior definition.
- Document upload size limit aligned between backend and docs.

Phase 1 Scope Boundary

Phase 1 includes:

- Entra/Bilko login and logout.
- Today dashboard and read-only invoice/expense lists.
- Receipt camera capture and expense attachment upload.
- Basic HR travel-order quick-add only if backend payload is confirmed.

Phase 1 excludes:

- Durable offline queue / SQLite sync.
- OCR extraction.
- Push notifications or push-token registration.
- Full `/mobile/*` BFF implementation unless separately scoped.
- Mobile regulatory e-invoice submission logic.

Consequences

- Mobile docs and the tech-stack spec must treat PWA notes as legacy/superseded for this workstream.
- Web Zustand stores can be mirrored/adapted, but not reused verbatim because mobile auth/storage differs.
- Existing `/api/v1/*` endpoints are preferred for Phase 1 where live; `/mobile/*` BFF is a Phase 2+ decision.
- Security review is required before production rollout because customer identity and financial data are involved.

Related Documents

- `docs/mobile/MOBILE-PRD.md`
- `docs/mobile/MOBILE-ARCHITECTURE.md`
- `docs/mobile/MOBILE-IMPL-SPEC-PHASE1.md`
- `/Users/makinja/system/specs/bilko-tech-stack.md`

Revision #1
Created 2026-06-07 19:43:25 UTC by John
Updated 2026-06-07 19:43:25 UTC by John