Bilko Mobile Entra Auth Bridge Spec

Bilko Mobile — Entra External ID Auth Bridge Spec

> **Status:** Phase 0 backend prerequisite
> **Date:** 2026-06-04
> **Related:** `docs/architecture/ADR-037-BILKO-MOBILE-NATIVE-ENTRA-AUTH.md`, `docs/mobile/MOBILE-IMPL-SPEC-PHASE1.md`

Purpose

Enable Bilko native mobile login for iPhone and Samsung/Android via Microsoft Entra External ID without relying on browser httpOnly refresh cookies.

The existing web cookie flow must remain intact until a separate web migration is explicitly approved.

Target Flow

1. Mobile app starts Microsoft Entra External ID login using OIDC Authorization Code + PKCE (`expo-auth-session`).
2. Mobile receives an Entra ID token / auth result.
3. Mobile calls Bilko backend auth bridge with the Entra token.
4. Backend validates Entra token issuer, audience, expiry, signature, and required claims using Entra JWKS.
5. Backend maps the external identity to Bilko `user`, `organization`, and role.
6. Backend issues Bilko API/session tokens suitable for React Native secure storage.
7. Mobile stores token/session material only in `expo-secure-store`.

Required Endpoints

`POST /api/v1/auth/entra/session`

Creates or resumes a Bilko session from a validated Entra identity.

Request:

```
{
  "idToken": "<entra-id-token>",
  "client": "mobile",
  "device": {
    "platform": "ios|android",
    "appVersion": "1.0.0"
  }
}
```

Response:

```
{
  "user": {
    "id": "uuid",
    "email": "user@example.com",
    "fullName": "Full Name",
    "role": "owner|admin|accountant|viewer"
  },
  "organization": {
    "id": "uuid",
    "name": "Company Name",
    "country": "HR|RS|BA",
    "baseCurrency": "EUR|RSD|BAM",
    "language": "hr|sr-Latn|sr-Cyrl|bs|en"
  },
  "tokens": {
    "accessToken": "<bilko-api-jwt>",
    "refreshToken": "<bilko-mobile-refresh-token>",
    "expiresIn": 900
  }
}
```

Rules:

- Do not set or require browser cookies for `client: mobile`.
- Do not accept unsigned/unverified JWTs.
- Do not trust email alone as identity key; store Entra issuer + subject/object ID mapping.
- If a matching Bilko user/org cannot be resolved, return an explicit onboarding/not-authorized error; do not silently create an organization.

`POST /api/v1/auth/mobile/refresh`

Refreshes Bilko API access token from a mobile refresh token stored in Keychain/Keystore.

Request:

```
{
  "refreshToken": "<bilko-mobile-refresh-token>"
}
```

Response:

```
{
  "accessToken": "<bilko-api-jwt>",
  "refreshToken": "<rotated-refresh-token>",
  "expiresIn": 900
}
```

Rules:

- Rotate refresh tokens.
- Reject reused/revoked refresh tokens.
- Bind refresh token to user/session/device metadata where feasible.
- Existing `POST /api/v1/auth/refresh` cookie flow may remain for web.

`POST /api/v1/auth/logout`

For mobile, revoke the current Bilko mobile refresh/session token and return success. Entra hosted session logout can be added later if required.

Data Model Requirements

At minimum, persist:

- Entra issuer (`iss`).
- Entra subject/object ID (`sub` / `oid`, exact claim depends on tenant config).
- Bilko user ID.
- Organization membership and role.
- Mobile refresh token hash, expiry, rotation family/session ID, device metadata, revoked timestamp.

Never store plaintext refresh tokens.

Configuration Requirements

Environment/config values:

- `ENTRA_EXTERNAL_ID_ISSUER`
- `ENTRA_EXTERNAL_ID_AUDIENCE`
- `ENTRA_EXTERNAL_ID_JWKS_URL`
- `ENTRA_EXTERNAL_ID_TENANT_ID` or equivalent tenant/domain identifier
- Allowed mobile redirect URIs for Expo dev/staging/production

No secrets should be committed to the repo.

Acceptance Criteria

Phase 0 is complete when:

- A real Entra test user can log in from an Expo iOS simulator build and receive Bilko `user`, `organization`, and tokens.
- The same flow works on Android emulator.
- Refresh works without browser cookies.
- Invalid issuer/audience/signature/expired token tests fail closed.
- A user with no Bilko org mapping receives a controlled not-authorized/onboarding response.
- Backend tests cover token validation, org/role mapping, refresh rotation, and logout/revocation.
- Web cookie-based login still passes existing tests.

Security Review Items

- Confirm Entra External ID tenant policy and MFA/passwordless settings.
- Confirm JWKS caching and key rotation handling.
- Confirm token TTLs and refresh-token max lifetime.
- Confirm logging does not include tokens or PII-heavy claims.

- Confirm Sentry/telemetry scrubbing for auth errors.

Revision #1
Created 2026-06-07 19:43:31 UTC by John
Updated 2026-06-07 19:43:31 UTC by John