ADR-037 -- Entra Authenticates, Bilko Authorises; Single-Role v1; Multi-Org Deferred

ADR-037 — Entra Authenticates, Bilko Authorises; Single-Role v1; Multi-Org Deferred

Field	Value
ADR number	ADR-037
Date	2026-06-08
Status	Accepted
Author	John (AI Director, ALAI Holding AS)
CEO decision	Alem Basic — confirmed 2026-06-07 (CEO resolution addendum, MC #103075)
Related MCs	MC #103075 (Entra migration plan), MC #103141–103146 (WP1–WP6 execution), MC #103089 (multi-org, parked)
Supersedes	Existing inline requireRole() pattern (pre-WP1)

Context

Bilko had a custom email/password authentication system and a simple numeric role hierarchy (`requireRole()` inline in route handlers). No permission catalog, no RBAC tables, no admin UI for user management. The CEO decision (June 2026) was to:

1. Replace email/password authentication with Microsoft Entra External ID (CIAM) — hard REPLACE, not phased coexist
2. Build a real permission-catalog RBAC system with a DB-backed role-to-permission mapping

Multiple design forks were evaluated by a multi-agent panel (Parisa Tabriz, Martin Kleppmann, Petter Graff, Bruce Momjian, Devils Advocate — MC #103075 forged prompt). Key unresolved tensions: web direct-bearer vs exchange, email-match JIT vs pre-provision-by-oid, roles-in-Entra-claims vs roles-in-Bilko-DB.

Decision

D1 — Identity Provider Boundary

Entra External ID (CIAM) authenticates. Bilko authorises.

- Entra issues tokens; Bilko backend validates JWKS RS256 signature, issuer, audience
- Bilko reads `oid` from the Entra token as the sole identity anchor (`sub` is pairwise-pseudonymous per app and must NOT be used)
- Bilko issues its own access + refresh tokens after Entra token exchange; downstream services consume Bilko tokens, not Entra tokens directly
- Role and permission data live in `users.role` + `role_permissions` (Bilko DB). No role or permission claims are read from Entra tokens

D2 — Single Role per User per Organisation (v1)

One role per user per org: `owner | admin | accountant | viewer`. The role is stored in `users.role` (single column). Multi-role per user and multi-org membership are explicitly deferred to a separate epic (MC #103089).

Rationale: zero live clients; single-org Entra tenant; keep scope tightly bounded; multi-org requires a `organization_members` join table and CIAM tenant model decisions that are not yet resolved.

D3 — Permission Catalog in DB; Flat Inheritance Seed

A `permissions` catalog table (52 keys, `resource:verb` format enforced by CHECK) and a `role_permissions` mapping table (V67) replace the inline `requireRole()` calls. Seed strategy: flat exhaustive rows per role (Strategy A) — no runtime hierarchy derivation. The seed exactly reproduces existing behaviour (no regression — verified by 204 RbacMatrixTest cases).

D4 — Live DB Permission Resolution; Fail-Closed

`PermissionService.resolve(role)` queries `role_permissions` at request time. Unknown role resolves to `emptySet()` (no permissions). `BilkoPrincipal` carries the resolved permission set. All route-level checks use `requirePermission("resource:verb")`.

D5 — Multi-Org Deferred

Entra CIAM is provisioned as a single tenant. JIT provisioning assigns a new Entra user to one Bilko organisation. Multi-org (one user in multiple orgs) requires: a `organization_members` join table, per-org permission resolution, and CIAM tenant model decisions. All deferred to MC #103089.

Consequences

Positive

- Authentication complexity moved to Microsoft (password policies, MFA, SSPR, account lifecycle)
- Bilko no longer stores password hashes for new users (`password_hash` is nullable)
- Permission model is auditable and admin-configurable without code changes (role-to-permission seed is data)
- Authz decisions are logged (`AuthzAuditLogger`) for incident investigation
- Admin UI for user + role management (no more raw SQL for role changes)

Negative / Trade-offs

- Entra CIAM has MAU-based pricing; cost gate was raised (OC#1, MC #103075) — free tier starts June 2026
- 7-day refresh token revocation window: a disabled Entra account remains valid in Bilko for up to 7 days (documented risk OC#4; mitigation: admin disables user in Bilko DB)
- Email-match JIT carries race risk if email is mutable or duplicated (martin-kleppmann + bruce-momjian dissent on record); serializable transaction is a partial mitigation; pre-provision-by-OID is the recommended production path
- Single-role v1 limits fine-grained delegation scenarios (e.g. "viewer + approve-only on specific documents") — documented as out of scope

Alternatives Considered

Alternative	Rejected reason
Roles in Entra claims (Entra app roles)	Couples authorisation to IdP; role changes require Entra admin action not Bilko admin action; prevents clean multi-IdP future. Rejected per petter-graff + parisa-tabriz panel consensus.
Phased coexist (email/password + Entra in parallel for 2+ weeks)	CEO confirmed hard REPLACE. Panel devils-advocate raised phased coexist as safer; CEO re-confirmed hard REPLACE given zero live users. AuthProvider interface (D5 MC #103075) technically enables a revert if needed.
Denormalised entra_oid on users table (bruce-momjian alternative)	Separate-table V64 model kept; enables multi-IdP future; join cost is negligible at current scale. Fork preserved but not resolved — separate-table remains.
ABAC / policy engine (v1)	Premature for current scale and requirements; adds complexity; deferred as explicit out-of-scope with comment in plan.

Open Decisions Not Resolved by This ADR

- **OC#4 — Refresh revalidation vs risk acceptance:** Option A (revalidate Entra account status on refresh, ~50ms) vs Option B (7-day window, documented risk). Requires CEO/Securion explicit decision. Code stub for Option A is in `AuthService.kt` referencing MC #103075.
- **OC#2 — Hard REPLACE confirmed** but AuthProvider interface (D5, MC #103075) enables reversion if needed.
- **Web direct-bearer vs mobile exchange (parisa-tabriz dissent LIVE):** Web: MSAL acquires Entra access token, sends as Bearer to API. Mobile: id_token exchange at `POST /auth/entra/session`. Web direct-bearer is implemented; exchange path preserved as commented stub per spec.

Document Links

- Bilko Authentication — Entra External ID (CIAM)
- Bilko RBAC — Users / Roles / Permissions
- Bilko Auth Migration Runbook + Admin Guide
- Source plan: `/Users/makinja/system/specs/bilko-web-entra-cutover-and-rbac-plan-2026-06-08.md`
- Forged prompt (panel dissent log): `/Users/makinja/system/prompts/forged/103075.md`
- Phase 0 config: `/tmp/evidence-103076/phase0-config.md`

Revision #1
Created 2026-06-08 07:43:19 UTC by John

Updated 2026-06-08 07:43:19 UTC by John