**Analyse platform**

Met recente wijzigingen – 23-10

2025-10-23T18:10:18.928Z

# **Inhoudsopgave**

# **1. Doel en doelgroep**

Dit document is bedoeld voor jou, een toekomstige Cursor-agent of ontwikkelaar, om het Appalti AI platform snel en correct te begrijpen en wijzigingen veilig door te voeren.

Focus: architectuur, flows, omgevingsvariabelen, endpoints, multi-tenant gedrag, e-mailverificatie, uitnodigingen en de laatste wijzigingen.

# **2. Snelle start (development)**

1) Vereiste env (voorbeeld, zie hoofdstuk 5 en 6):

MONGODB\_URI, MONGODB\_DB, NEXTAUTH\_SECRET, AUTH0\_CLIENT\_ID, AUTH0\_CLIENT\_SECRET, AUTH0\_ISSUER\_BASE\_URL, REQUIRE\_VERIFIED\_EMAIL=1

GRAPH\_TENANT\_ID, GRAPH\_CLIENT\_ID, GRAPH\_CLIENT\_SECRET, (optioneel GRAPH\_MAIL\_\*), GRAPH\_FROM\_EMAIL of EMAIL\_FROM

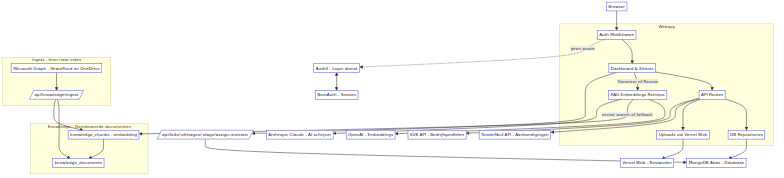
OPENAI\_API\_KEY, (OPENAI\_EMBEDDING\_MODEL), Upstash Redis voor rate limit (optioneel)

2) Run: npm run dev (Next.js 15, App Router).

3) Login: Auth0 Universal Login. Eerste login synchroniseert user + memberships; Appalti-accounts (@appalti.nl) worden automatisch aan de Appalti-company toegevoegd.

# **3. Architectuuroverzicht**

Next.js (App Router) + NextAuth (Auth0) + MongoDB Atlas. Integraties: Microsoft Graph (mail + files), KVK, TenderNed, @vercel/blob, Upstash (rate limiting), Sentry, AI: OpenAI (embeddings) + Anthropic (generatie/review).



# **4. Authenticatie, sessies en middleware**

Bronnen: src/lib/auth.ts, middleware.ts, src/lib/auth/context.ts

- NextAuth v5 (Auth0). Sessiestrategie: database via MongoDB adapter.

- callbacks.session verrijkt sessie met: user.id, isAppaltiUser (domeincheck), memberships → tenantId/companyId/rollen.

- callbacks.signIn: user sync (create/update), emailVerified uit Auth0 claim, optioneel blokkeren bij REQUIRE\_VERIFIED\_EMAIL=1.

- Appalti e-mails worden (idempotent) lid van de Appalti-company.

- middleware.ts: redirect naar /auth/signin als niet ingelogd (uitzonderingen: auth, api/auth, static, /).

# **5. Omgevingsvariabelen (minimaal)**

- MONGODB\_URI, MONGODB\_DB

- NEXTAUTH\_SECRET, AUTH0\_CLIENT\_ID, AUTH0\_CLIENT\_SECRET, AUTH0\_ISSUER\_BASE\_URL

- REQUIRE\_VERIFIED\_EMAIL=1 (om niet-geverifieerde logins te weigeren)

- GRAPH\_TENANT\_ID, GRAPH\_CLIENT\_ID, GRAPH\_CLIENT\_SECRET (Graph API)

- GRAPH\_FROM\_EMAIL of EMAIL\_FROM (afzender voor e-mail)

- OPENAI\_API\_KEY (embeddings)

- (Optioneel) GRAPH\_MAIL\_\* voor gescheiden mail-credentials; Upstash Redis tokens; Sentry project tokens; Vercel Blob secrets.

# **6. Multi-tenancy en rollen**

Memberships koppelen users ↔ companies met tenantId en rollen. Helpers: requireAuth, requireCompanyRole, requirePlatformRole.

Actieve context kan via cookies: activeCompanyId/activeTenantId (wisselen via POST /api/auth/switch-tenant).

Company roles: viewer < member < admin < owner. Platform roles (Appalti): viewer, support, admin, super\_admin.

# **7. Datamodel en repositories**

Kerncollecties: companies, users, memberships, clientCompanies, tenders, bids (stages). RAG: knowledge\_documents, knowledge\_chunks.

Repositories bevatten indices en tenant-scoping. Zie src/lib/db/repositories/\*.

# **8. Belangrijke API endpoints (selectie)**

- Auth: GET /api/auth/me; POST /api/auth/registration (create-company, join-company, request-domain-join); POST /api/auth/switch-tenant

- Memberships: POST /api/memberships/invite, POST /api/memberships/accept, GET /api/memberships/invite-info

- Clients: GET/POST /api/clients, GET/PUT/DELETE /api/clients/[id], IKP routes

- Knowledge: ingest en search; Bids/Tenders: stages, AI generate/review, uploads

# **9. Uitnodigingen en registratie**

Flow:

1) Admin nodigt uit via POST /api/memberships/invite (domein-whitelist afdwinging indien geconfigureerd).

2) E-mail wordt verstuurd via Microsoft Graph met invite-token link naar /invite?token=...

3) /invite probeert de uitnodiging te accepteren via POST /api/memberships/accept; mismatch van e‑mail toont wissel/registratie-opties.

4) /auth/signup ondersteunt prefill (screen\_hint, login\_hint).

Alternatief: POST /api/auth/registration met action=request-domain-join stuurt owners een notificatie bij domeinmatch.

# **10. Microsoft Graph en e-mail**

Tokens worden gecached (getGraphAccessToken/getGraphMailAccessToken). E-mail versturen via /users/{from}/sendMail met HTML-templates (invite & owner-approval).

# **11. RAG/AI en ingest**

OpenAI embeddings (text-embedding-3-small standaard). RAG zoekt in knowledge\_chunks met Atlas Vector Search (of cosine fallback). Ingest haalt tekstachtige documenten via Graph, chunked + embedded opslaan.

# **12. Observability en limiting**

Sentry integratie aanwezig. Upstash Redis rate limiting voor gevoelige endpoints (o.a. invites, KVK).

# **13. Beveiliging & aandachtspunten**

- Zet REQUIRE\_VERIFIED\_EMAIL=1 in productie.

- Respecteer domein-whitelist per company bij invites/join.

- Middleware uitsluitingen niet te ruim zetten.

- Geen productiebuilds blokkeren op lint/type (next.config.ts negeert fouten); herstel dit indien nodig.

# **14. Recente wijzigingen (tot 23-10, laatste commit 2025‑10‑21)**

- fix(invite-accept): verbeterde e‑mail case handling en foutmeldingen (403 bij mismatch, 400 bij verlopen token).

- Nieuwe endpoint GET /api/memberships/invite-info voor UI-branding en validatie. /auth/signup pagina toegevoegd (invite‑based signup).

- Invite endpoint fallback naar actieve company; domein-whitelist afdwingen; Graph-mail met nette HTML.

- Registration API: acties create-company, join-company (invite token + whitelist), nieuw request-domain-join → owners e‑mail notificatie via Graph.

- UserRepository: betere update bij herlogin (naam, avatar, emailVerified). Graph token functies opgesplitst voor mail.

- CURSOR\_README en ARCHITECTURE\*.md gefinetuned (Mermaid fixes, A2/A4 beelden toegevoegd).

# **15. Runbook – handmatige testcases**

1) Login met geverifieerde e‑mail; bij REQUIRE\_VERIFIED\_EMAIL=1 moet on‑geverifieerd falen (redirect naar /auth/error?error=Verification).

2) Invite flow: als ADMIN start POST /api/memberships/invite → bekijk mail → open /invite?token=... → accepteer; valideer membership en cookies; redirect naar /dashboard.

3) Mismatch e‑mail bij accept: UI toont “wissel van account” en link naar /auth/signup met voorgevulde e‑mail.

4) request-domain-join: POST /api/auth/registration met action=request-domain-join → owners ontvangen notificatie → nodigen vervolgens uit via Team.

5) RAG: test /api/knowledge/ingest (run-defaults) en AI generate/review endpoints; zonder Vector Index zie je fallback melding.

# **16. Nuttige paden en bestanden**

• Auth: src/lib/auth.ts, middleware.ts, src/lib/auth/context.ts

• Repos: src/lib/db/repositories/\*, Modellen: src/lib/db/models/\*

• Invites & registratie: src/app/api/memberships/\*, src/app/api/auth/registration/\*, pages: /auth/signup, /invite

• RAG & ingest: src/lib/rag.ts, src/app/api/knowledge/\*

• Graph & mail: src/lib/graph.ts, src/lib/email.ts

• KVK/TenderNed: src/lib/kvk-api.ts, src/lib/tenderned\*.ts, bijbehorende API routes

# **17. Appendix – versies en build**

Next 15.4.5, React 19.1, NextAuth 5 beta. TypeScript strict. ESLint 9. Tailwind 4. Build negeert lint/TS‑errors in next.config.ts.