

# AdvanDEB Platforma

## Plan Razvoja

### Faza 0: Upravljanje Korisnicima i Autentifikacija

Verzija 3.0 - Arhitektura Temeljena na Sposobnostima

AdvanDEB Razvojni Tim

12. prosinca 2025.

#### Abstract

Ovaj dokument predstavlja sveobuhvatni plan razvoja AdvanDEB platforme, integriranog sustava za upravljanje biološkim znanjem i modeliranje temeljeno na jedinkama (IBM). Platforma se sastoji od dvije glavne komponente: Knowledge Builder za unos i upravljanje znanjem te Modeling Assistant za potporu IBM modeliranju. Ovaj izvještaj fokusira se na implementaciju Faze 0: uspostavljanje platformске autentifikacije, upravljanja korisnicima i infrastrukture za autorizaciju koristeći pojednostavljeni model uloga temeljen na sposobnostima.

# Contents

<b>1</b>	<b>Izvršni Sažetak</b>	<b>4</b>
1.1	Pregled Projekta	4
1.2	Trenutna Faza Razvoja	4
1.3	Ključna Arhitektonska Odluka: Pojednostavljenje v3.0	4
<b>2</b>	<b>Arhitektura Sustava</b>	<b>4</b>
2.1	Komponente Platforme	4
2.1.1	advandeb-shared-utils	4
2.1.2	Knowledge Builder	5
2.1.3	Modeling Assistant	5
2.2	Arhitektura Autentifikacije	5
2.2.1	Jedinstvena Prijava (SSO)	5
2.2.2	Metode Autentifikacije	5
2.2.3	Platformska Baza Korisnika	5
<b>3</b>	<b>Model Uloga i Dozvola v3.0</b>	<b>6</b>
3.1	Osnovne Uloge	6
3.1.1	Administrator	6
3.1.2	Kustos Znanja	6
3.1.3	Istraživač Znanja	7
3.2	Radni Proces Zahtjeva za Sposobnosti	7
3.2.1	Novi Korisnik - Zahtjev za Osnovnu Ulogu	7
3.2.2	Postojeći Kustos - Zahtjev za Sposobnost	7
3.3	Razrješavanje Dozvola	8
<b>4</b>	<b>Trenutna Faza: Plan Razvoja Faze 0</b>	<b>8</b>
4.1	Pregled Faze	8
4.2	Plan Implementacije	8
4.2.1	Faza 1: Temelj	8
4.2.2	Faza 2: Backend Upravljanja Korisnicima	9
4.2.3	Faza 3: Integracija Frontenda	9
4.2.4	Faza 4: Radni Proces Recenzije	10
4.2.5	Faza 5: Day Zero i Migracija	10
4.2.6	Faza 6: MA Integracija i Dotjerivanje	11
<b>5</b>	<b>Tehnički Detalji Implementacije</b>	<b>11</b>
5.1	Shema Baze Podataka	11
5.1.1	users Kolekcija	11
5.1.2	capability_requests Kolekcija	12
5.1.3	api_keys Kolekcija	12
5.1.4	audit_logs Kolekcija	13
5.2	API Krajnje Točke	13
5.2.1	Rute Autentifikacije	13
5.2.2	Rute Upravljanja Korisnicima	13
5.2.3	Rute Zahtjeva za Sposobnosti	13
5.2.4	Rute API Ključeva	14
5.2.5	Rute Recenzije	14

5.3	Sigurnosne Razmatranja . . . . .	14
5.3.1	Sigurnost Tokena . . . . .	14
5.3.2	Sigurnost API Ključeva . . . . .	14
5.3.3	Ograničavanje Stope . . . . .	14
5.3.4	Revizijsko Bilježenje . . . . .	15
<b>6</b>	<b>Strategija Testiranja</b>	<b>15</b>
6.1	Jedinični Testovi . . . . .	15
6.2	Integracijski Testovi . . . . .	15
6.3	End-to-End Testovi . . . . .	15
6.4	Sigurnosno Testiranje . . . . .	16
<b>7</b>	<b>Plan Postavljanja</b>	<b>16</b>
7.1	Razvojno Okruženje . . . . .	16
7.2	Staging Okruženje . . . . .	16
7.3	Produksijsko Okruženje . . . . .	16
<b>8</b>	<b>Procjena Rizika</b>	<b>17</b>
8.1	Tehnički Rizici . . . . .	17
8.1.1	Rizik: Kompleksna Logika Dozvola . . . . .	17
8.1.2	Rizik: Problemi OAuth Integracije . . . . .	17
8.1.3	Rizik: Uska Grla Performansi . . . . .	17
8.2	Projektni Rizici . . . . .	17
8.2.1	Rizik: Povećanje Opsega . . . . .	17
8.2.2	Rizik: Zakašnjenja Projekta . . . . .	18
<b>9</b>	<b>Kriteriji Uspjeha</b>	<b>18</b>
<b>10</b>	<b>Sljedeće Faze</b>	<b>18</b>
10.1	Faza 1: Stabilizacija Knowledge Buildera . . . . .	18
10.2	Faza 2: Prototip Modeling Assistanta . . . . .	19
10.3	Faza 3: Poboljšana Integracija i UX . . . . .	19
10.4	Faza 4: Proširenja i Dodaci . . . . .	19
<b>11</b>	<b>Zaključak</b>	<b>19</b>

# 1 Izvršni Sažetak

## 1.1 Pregled Projekta

AdvanDEB platforma je sveobuhvatni sustav dizajniran za potporu biološkim istraživanjima kroz upravljanje znanjem i modeliranje temeljeno na jedinkama. Platforma integrira dvije ključne komponente:

- **Knowledge Builder (KB):** FastAPI + Vue.js sustav za unos, obradu i upravljanje biološkim znanjem iz literature, web izvora i strukturiranih podataka
- **Modeling Assistant (MA):** Specijalizirana komponenta za pretraživanje znanja i zaključivanje u svrhu potpore radnim procesima modeliranja temeljenog na jedinkama

## 1.2 Trenutna Faza Razvoja

Projekt je trenutno u **Fazi 0: Upravljanje Korisnicima i Autentifikacija**. Ova temeljna faza uspostavlja sigurnost, kontrolu pristupa i infrastrukturu za suradnju potrebnu za sve buduće mogućnosti platforme.

## 1.3 Ključna Arhitektonska Odluka: Pojednostavljenje v3.0

Nakon početnih iteracija dizajna (v1.0 i v2.0), arhitektura je pojednostavljena na model temeljen na sposobnostima:

- **Od:** 6 različitih uloga (Administrator, Kustos Znanja, Recenzent Znanja, Operator Agent, Analitičar Podataka, Istraživač Znanja)
- **Do:** 3 osnovne uloge (Administrator, Kustos Znanja, Istraživač Znanja) + 3 opcionalne sposobnosti (Pristup Agentima, Analitički Pristup, Status Recenzenta)

Ovo pojednostavljenje eliminira redundanciju uloga uz održavanje svih funkcionalnih zahtjeva kroz fleksibilniji model dozvola.

# 2 Arhitektura Sustava

## 2.1 Komponente Platforme

### 2.1.1 advandeb-shared-utils

Python paket koji pruža dijeljene uslužne programe za autentifikaciju i autorizaciju, eliminirajući dupliciranje koda između backend komponenti. Sadrži:

- Generiranje i validaciju JWT tokena
- Upravljanje API ključevima
- Logiku provjere dozvola
- Modele korisnika (Pydantic)
- Uslužne programe za revizijsko bilježenje
- Pomoćnike za Google OAuth integraciju

### 2.1.2 Knowledge Builder

**Primarni pružatelj autentifikacije** za platformu. Sadrži:

- Google OAuth 2.0 krajnje točke
- Sučelje za upravljanje korisnicima
- Radne procese za odobravanje uloga i sposobnosti
- Unos i obradu znanja
- Okvir AI agenata za automatiziranu ekstrakciju
- Konstrukciju grafa znanja

### 2.1.3 Modeling Assistant

Dijeli infrastrukturu autentifikacije s Knowledge Builderom:

- Isti JWT tokeni vrijede za obje komponente
- Ista baza korisnika (MongoDB)
- Pretraživanje znanja iz KB podataka
- Sučelje za izgradnju scenarija
- Podrška za sastavljanje modela i simulaciju

## 2.2 Arhitektura Autentifikacije

### 2.2.1 Jedinstvena Prijava (SSO)

Korisnici se autentificiraju jednom putem Google OAuth 2.0 i dobivaju JWT tokene važeće za cijelu platformu. Iste vjerodajnice omogućuju pristup i Knowledge Builderu i Modeling Assistantu bez zasebne autentifikacije.

### 2.2.2 Metode Autentifikacije

1. **Google OAuth 2.0:** Primarna metoda za korisnike web sučelja
2. **API Ključevi:** Za programski pristup, s opsegom temeljenim na sposobnostima
3. **JWT Tokeni:** Kratkoživući pristupni tokeni (1 sat) + tokeni za osvježavanje (30 dana)

### 2.2.3 Platformska Baza Korisnika

Jedna MongoDB baza pohranjuje sve podatke vezane uz korisnike:

- `users` kolekcija - Korisnički profili s `base_role` i `capabilities`
- `capability_requests` kolekcija - Radni procesi za odobravanje osnovnih uloga i sposobnosti
- `api_keys` kolekcija - API ključevi važeći za cijelu platformu
- `audit_logs` kolekcija - Potpuni revizijski trag za sve komponente

## 3 Model Uloga i Dozvola v3.0

### 3.1 Osnovne Uloge

#### 3.1.1 Administrator

**Svrha:** Sistemska ovlast i konfiguracija platforme

**Dozvole:**

- Potpuni pristup sustavu svim komponentama
- Upravljanje korisnicima (odobravanje uloga i sposobnosti)
- Konfiguracija sustava
- Unos početnog znanja (Day Zero)
- Poništavanje bilo koje odluke recenzije
- Pristup svim revizijskim zapisima

#### 3.1.2 Kustos Znanja

**Svrha:** Kreator sadržaja i stručnjak domene

**Osnovne Dozvole:**

- Učitavanje dokumenata (pojedinačno i grupno)
- Kreiranje činjenica i stiliziranih činjenica
- Izgradnja grafova znanja
- Kreiranje scenarija i modela (u MA)
- Uređivanje vlastitih doprinosa
- Pregled objavljenog znanja

**Opcionalne Sposobnosti** (moraju se zatražiti i odobriti):

- **Pristup Agentima:** Pokretanje AI agenata, korištenje prilagođenih alata, pregled zapisa agenata
- **Analitički Pristup:** Napredni upiti, masovni izvoz, generiranje API ključeva
- **Status Recenzenta:** Pristup redu za recenziju, odobravanje/odbijanje znanja, kontrola kvalitete

### 3.1.3 Istraživač Znanja

**Svrha:** Korisnik samo za čitanje za pregledavanje znanja

**Dozvole:**

- Pregledavanje i pretraživanje objavljenog znanja
- Pregled grafova znanja
- Pregled objavljenih modela i scenarija (u MA)
- Kreiranje privatnih bilješki
- Izvoz ograničenih skupova podataka (za osobnu uporabu)
- Spremanje upita za pretraživanje

## 3.2 Radni Proces Zahtjeva za Sposobnosti

### 3.2.1 Novi Korisnik - Zahtjev za Osnovnu Ulogu

1. Korisnik se prijavljuje putem Googlea
2. Status: `pending_approval`, `base_role`: `null`
3. Korisnik ispunjava obrazac za zahtjev uloge (odabir Kustos ili Istraživač)
4. Navodi pripadnost, područje istraživanja, obrazloženje
5. Administrator pregleda i odobrava/odbija
6. Korisnik prima obavijest e-mailom
7. Pristup dodijeljen na temelju odobrene osnovne uloge

### 3.2.2 Postojeći Kustos - Zahtjev za Sposobnost

1. Kustos se prijavljuje s osnovnim pristupom
2. Stranica profila prikazuje "Zatraži dodatne sposobnosti"
3. Korisnik odabire željene sposobnosti:
  - Pristup Agentima
  - Analitički Pristup
  - Status Recenzenta
4. Navodi obrazloženje za svaku sposobnost
5. Administrator pregleda
6. Sposobnosti dodane korisničkom profilu
7. Korisnik odmah dobiva nove dozvole

### 3.3 Razrješavanje Dozvola

Dozvole se izračunavaju na temelju:

$$\text{Korisničke Dozvole} = \text{Dozvole Osnovne Uloge} \cup \text{Dozvole Sposobnosti} \quad (1)$$

**Primjeri:**

- Kustos (samo osnovna): Može kreirati/uređivati znanje
- Kustos + Pristup Agentima: Može kreirati znanje i pokretati agente
- Kustos + Analitički Pristup + Status Recenzenta: Može kreirati, izvoziti i recenzirati
- Administrator: Ima sve dozvole neovisno o sposobnostima

## 4 Trenutna Faza: Plan Razvoja Faze 0

### 4.1 Pregled Faze

**Cilj:** Uspostaviti potpunu infrastrukturu za autentifikaciju, autorizaciju i upravljanje korisnicima za cijelu AdvanDEB platformu.

**Ishod:** Potpuno autentificirana platforma s 3 osnovne uloge + 3 sposobnosti, jedinstvena prijava kroz KB i MA, Google OAuth integracija, API ključevi, radni proces recenzije znanja i mogućnost Day Zero unosa.

### 4.2 Plan Implementacije

#### 4.2.1 Faza 1: Temelj

**Fokus:** Backend sustav autentifikacije

**Zadaci:**

1. Kreirati `advandeb-shared-utils` repozitorij i strukturu paketa
2. Implementirati generiranje i validaciju JWT tokena
3. Implementirati Google OAuth 2.0 klijent
4. Kreirati User, CapabilityRequest, APIKey, AuditLog modele (Pydantic)
5. Implementirati funkcije provjere dozvola (`has_base_role`, `has_capability`)
6. Postaviti uslužne programe za MongoDB vezu
7. Kreirati funkcije za revizijsko bilježenje
8. Napisati jedinične testove za uslužne programe autentifikacije
9. Postaviti CI/CD za dijeljeni paket

**Ishod:** Funkcionalni `advandeb-shared-utils` paket spreman za integraciju



### 4.2.2 Faza 2: Backend Upravljanja Korisnicima

**Fokus:** Integracija Knowledge Builder backenda

**Zadaci:**

1. Dodati `advandeb-shared-utils` zavisnost KB backendu
2. Kreirati `/auth` usmjerivač (prijava, povratni poziv, odjava, osvježavanje)
3. Kreirati `/users` usmjerivač (profil, ažuriranje)
4. Kreirati `/capability-requests` usmjerivač (kreiranje, lista, odobravanje/odbijanje)
5. Kreirati `/api-keys` usmjerivač (generiranje, lista, opoziv)
6. Implementirati `AuthMiddleware` za sve postojeće rute
7. Implementirati `RateLimiter` middleware
8. Implementirati `AuditLogger` middleware
9. Kreirati `UserService`, `RoleService`, `APIKeyService`
10. Postaviti MongoDB kolekcije: `users`, `capability_requests`, `api_keys`, `audit_logs`
11. Konfigurirati Google OAuth vjerodajnice
12. Implementirati sustav obavijesti e-mailom

**Ishod:** Potpuno funkcionalni backend za autentifikaciju i upravljanje korisnicima

### 4.2.3 Faza 3: Integracija Frontenda

**Fokus:** Knowledge Builder frontend

**Zadaci:**

1. Kreirati Login View s Google OAuth gumbom
2. Kreirati Profile View (prikaz informacija korisnika, osnovne uloge, sposobnosti)
3. Kreirati Role Request View (za nove korisnike)
4. Kreirati Capability Request View (za postojeće kustose)
5. Kreirati Administrator Dashboard (lista korisnika, zahtjevi na čekanju)
6. Kreirati API Key Management View (generiranje, pregled, opoziv)
7. Implementirati Auth Store (Pinia/Vuex) s upravljanjem tokenima
8. Dodati Axios presretače za ubacivanje JWT tokena
9. Dodati automatsku logiku osvježavanja tokena
10. Ažurirati sve postojeće prikaze s renderiranjem temeljenim na dozvolama
11. Dodati rukovanje greškama za 401/403 odgovore
12. Implementirati upite "Zatraži pristup" za nedostatne dozvole

**Ishod:** Potpuni autentificirani frontend s jedinstvenom prijavom

#### 4.2.4 Faza 4: Radni Proces Recenzije

**Fokus:** Sustav validacije znanja

**Zadaci:**

1. Dodati `status` polje svim entitetima znanja (`facts`, `stylized_facts`, `graphs`, `documents`)
2. Implementirati prijelaze statusa: `draft` → `pending_review` → `published/rejected/changes_requested`
3. Kreirati `/reviews` usmjerivač (`red`, `odobranje`, `odbijanje`, `zahtjev-izmjena`)
4. Kreirati `ReviewService` s poslovnom logikom
5. Kreirati `Review Queue View` (za korisnike sa Status Recenzenta)
6. Dodati značke statusa prikazima liste znanja
7. Implementirati logiku dodjele recenzenata
8. Dodati praćenje povijesti recenzija
9. Kreirati nadzornu ploču recenzenta sa statistikom
10. Dodati obavijesti e-mailom za promjene statusa recenzije
11. Spriječiti samo-recenziju (korisnici ne mogu recenzirati vlastite doprinose)

**Ishod:** Funkcionalni sustav peer recenzije za kontrolu kvalitete znanja

#### 4.2.5 Faza 5: Day Zero i Migracija

**Fokus:** Početni unos znanja i migracija podataka

**Zadaci:**

1. Kreirati Day Zero radni proces grupnog unosa
2. Dodati `is_day_zero` oznaku entitetima znanja
3. Implementirati krajnje točke za kreiranje Day Zero (samo admin)
4. Dodati značke "Temeljno Znanje" u korisničkom sučelju
5. Migrirati postojećih 1.300 PDF-ova iz `/papers` direktorija
6. Kreirati skriptu za migraciju za naslijeđene podatke
7. Dodati metapodatke o pripisivanju migriranom sadržaju
8. Auto-odobranje Day Zero sadržaja (preskakanje recenzije)
9. Kreirati nadzornu ploču za upravljanje Day Zero
10. Dodati grupno označavanje za Day Zero sadržaj
11. Testirati i validirati sve migrirane podatke

**Ishod:** Platforma popunjena temeljnim znanjem, naslijeđeni podaci migrirani

### 4.2.6 Faza 6: MA Integracija i Dotjerivanje

**Fokus:** Autentifikacija Modeling Assistanta i završno testiranje

**Zadaci:**

1. Dodati `advandeb-shared-utils` zavisnost MA backendu
2. Implementirati middleware za autentifikaciju u MA koristeći dijeljenu biblioteku
3. Dodati JWT validaciju tokena svim MA rutama
4. Implementirati provjere dozvola za MA-specifične operacije (kreiranje scenarija, pokretanje simulacija)
5. Ažurirati MA frontend za korištenje dijeljenog Auth Store
6. Testirati međukomponentnu autentifikaciju (KB → MA s istim tokenom)
7. Dodati polje komponente revizijskim zapisima ("knowledge\_builder" vs "modeling\_assistant")
8. Kreirati sveobuhvatne integracijske testove
9. Izvršiti sigurnosnu reviziju (istek tokena, granice dozvola, ograničavanje stope)
10. Testiranje opterećenja (autentificirati 100+ istovremenih korisnika)
11. Napisati korisničku dokumentaciju (vodič za autentifikaciju, vodič za zahtjev sposobnosti)
12. Napisati administratorsku dokumentaciju (upravljanje korisnicima, radni procesi odobravanja)
13. Napisati razvojnu dokumentaciju (dodavanje novih dozvola, proširivanje sposobnosti)
14. Završne popravke grešaka i dotjerivanje

**Ishod:** Jedinstvena platforma s potpunom autentifikacijom kroz KB i MA

## 5 Tehnički Detalji Implementacije

### 5.1 Shema Baze Podataka

#### 5.1.1 users Kolekcija

```
{
  "_id": ObjectId,
  "google_id": string,           // Jedinstveni
  "email": string,
  "name": string,
  "picture_url": string,
  "base_role": string,          // "administrator", "knowledge_curator",
                                // "knowledge_explorator"
  "capabilities": [string],      // ["agent_access", "analytics_access",
                                // "reviewer_status"]
  "status": string,              // "active", "suspended", "pending_approval"
```

```
"created_at": datetime,
"updated_at": datetime,
"last_login": datetime,
"login_count": int,
"metadata": {
    "affiliation": string,
    "research_area": string,
    "orcid": string
}
}
```

### 5.1.2 capability\_requests Kolekcija

```
{
    "_id": ObjectId,
    "user_id": ObjectId,
    "request_type": string,          // "base_role" ili "capability"

    // Za zahtjeve osnovne uloge
    "requested_base_role": string,
    "current_base_role": string,

    // Za zahtjeve sposobnosti
    "requested_capabilities": [string],
    "current_capabilities": [string],

    "justification": string,
    "form_data": dict,
    "status": string,               // "pending", "approved", "rejected"
    "created_at": datetime,
    "reviewed_by": ObjectId,
    "reviewed_at": datetime,
    "review_notes": string
}
```

### 5.1.3 api\_keys Kolekcija

```
{
    "_id": ObjectId,
    "user_id": ObjectId,
    "key_hash": string,             // SHA-256 običnog ključa
    "key_prefix": string,          // "advk_abc12345"
    "name": string,
    "scopes": [string],            // Auto-dodijeljeno na temelju
                                   // base_role + capabilities korisnika
    "status": string,              // "active", "revoked", "expired"
    "created_at": datetime,
    "expires_at": datetime,
    "last_used_at": datetime,
```

```
"rate_limit": {
  "requests_per_minute": int,
  "requests_per_day": int
}
```

#### 5.1.4 audit\_logs Kolekcija

```
{
  "_id": ObjectId,
  "user_id": ObjectId,
  "action": string,           // "create_fact", "approve_knowledge", itd.
  "resource_type": string,    // "fact", "document", "scenario", itd.
  "resource_id": ObjectId,
  "component": string,        // "knowledge_builder" ili "modeling_assistant"
  "details": dict,
  "ip_address": string,
  "user_agent": string,
  "auth_method": string,      // "jwt", "api_key"
  "timestamp": datetime
}
```

## 5.2 API Krajnje Točke

### 5.2.1 Rute Autentifikacije

- GET /auth/login - Preusmjeravanje na Google OAuth
- GET /auth/callback - Rukovatelj povratnog poziva OAuth
- POST /auth/logout - Poništavanje tokena
- POST /auth/refresh - Osvježavanje pristupnog tokena

### 5.2.2 Rute Upravljanja Korisnicima

- GET /users/me - Dohvati trenutni korisnički profil
- PATCH /users/me - Ažuriraj profil
- GET /users - Lista korisnika (samo admin)
- GET /users/:id - Dohvati detalje korisnika (samo admin)

### 5.2.3 Rute Zahtjeva za Sposobnosti

- POST /capability-requests - Kreiraj novi zahtjev
- GET /capability-requests - Lista vlastitih zahtjeva
- GET /capability-requests/pending - Lista na čekanju (samo admin)
- POST /capability-requests/:id/approve - Odobri (samo admin)

- POST /capability-requests/:id/reject - Odbij (samo admin)

#### 5.2.4 Rute API Ključeva

- POST /api-keys - Generiraj novi ključ
- GET /api-keys - Lista vlastitih ključeva
- DELETE /api-keys/:id - Opozovi ključ

#### 5.2.5 Rute Recenzije

- GET /reviews/queue - Stavke na čekanju za recenziju (zahtijeva Status Recenzenta)
- POST /reviews/:id/approve - Odobri znanje
- POST /reviews/:id/reject - Odbij znanje
- POST /reviews/:id/request-changes - Zatraži izmjene

### 5.3 Sigurnosne Razmatranja

#### 5.3.1 Sigurnost Tokena

- JWT tajni ključ: 256-bitna slučajna vrijednost pohranjena u okolini
- Pristupni tokeni: Kratkoživući (1 sat) za ograničavanje prozora izloženosti
- Tokeni za osvježavanje: Dugoživući (30 dana) ali sigurno pohranjeni
- Rotacija tokena pri osvježavanju za sprječavanje napada ponavljanja
- JTI (JWT ID) za mogućnost opoziva tokena

#### 5.3.2 Sigurnost API Ključeva

- SHA-256 hash prije pohrane (obični ključ se nikad ne pohranjuje)
- Identifikacija temeljena na prefiksu (advk...) za brzo pretraživanje
- Ograničavanje stope: 200-500 zahtjeva/minutu ovisno o sposobnostima
- Automatski istek (30-90 dana)
- Podrška za bijelu listu IP adresa (opcionalno)

#### 5.3.3 Ograničavanje Stope

- Ograničenja po korisniku temeljena na sposobnostima
- Redis-bazirani algoritam token bucket
- Ograničenja: Istraživač (100 zah/min), Kustos (200 zah/min), Kustos+Analitika (500 zah/min)
- Dnevna ograničenja za grupne operacije

### 5.3.4 Revizijsko Bilježenje

- Sve operacije pisanja zabilježene
- Svi događaji autentifikacije zabilježeni
- Sve promjene dozvola zabilježene
- Nepromjenjivi zapisi (samo dodavanje)
- Zadržavanje: minimalno 2 godine

## 6 Strategija Testiranja

### 6.1 Jedinični Testovi

- Sve funkcije u `advandeb-shared-utils`
- Generiranje i validacija JWT
- Logika provjere dozvola
- Hash i validacija API ključeva
- Ciljana pokrivenost: 90%+

### 6.2 Integracijski Testovi

- Potpuni tokovi autentifikacije (OAuth, JWT, API ključevi)
- Međukomponentna autentifikacija (KB  $\rightarrow$  MA)
- Provođenje dozvola na svim zaštićenim rutama
- Radni proces zahtjeva za sposobnosti
- Radni proces recenzije

### 6.3 End-to-End Testovi

- Registracija korisnika kroz odobrenje
- Kustos zahtjeva sposobnosti
- Kreiranje znanja i recenzija
- Međukomponentni pristup (kreiranje u KB, pregled u MA)

## 6.4 Sigurnosno Testiranje

- Pokušaj pristupa bez autentifikacije
- Pokušaj eskalacije privilegija
- Validacija isteka tokena
- Provođenje ograničavanja stope
- Pokušaji SQL injekcije (iako se koristi MongoDB)
- Testiranje XSS ranjivosti

## 7 Plan Postavljanja

### 7.1 Razvojno Okruženje

- Lokalna MongoDB instanca
- Lokalni Ollama za LLM funkcionalnost
- Google OAuth testne vjerodajnice
- Lažni servis za e-mail

### 7.2 Staging Okruženje

- Hostirana MongoDB (Atlas)
- Postavljeni backend (Docker kontejneri)
- Postavljeni frontend (Nginx)
- Prave Google OAuth vjerodajnice (testna domena)
- Pravi servis za e-mail (SendGrid/Mailgun)

### 7.3 Produkcijsko Okruženje

- Proizvodni MongoDB klaster (replica set)
- Redis klaster za ograničavanje stope
- Opterećenjem balansirani backend serveri
- CDN za frontend resurse
- SSL/TLS certifikati
- Sigurnosna kopija i oporavak od katastrofe
- Praćenje i upozoravanje



## 8 Procjena Rizika

### 8.1 Tehnički Rizici

#### 8.1.1 Rizik: Kompleksna Logika Dozvola

Vjerojatnost: Srednja

Utjecaj: Visok

Ublažavanje:

- Sveobuhvatni jedinični testovi za funkcije dozvola
- Dokumentacija matrice dozvola
- Fokus pregleda koda na autorizacijskom kodu

#### 8.1.2 Rizik: Problemi OAuth Integracije

Vjerojatnost: Niska

Utjecaj: Visok

Ublažavanje:

- Rano integracijske testiranje
- Alternativa email/lozinka autentifikacija ako je potrebno
- Dobro dokumentirana OAuth konfiguracija

#### 8.1.3 Rizik: Uska Grla Performansi

Vjerojatnost: Srednja

Utjecaj: Srednji

Ublažavanje:

- Testiranje opterećenja tijekom završnih faza
- Redis cache za često pristupane podatke
- Indeksiranje baze na pretragama korisnika

### 8.2 Projektni Rizici

#### 8.2.1 Rizik: Povećanje Opsega

Vjerojatnost: Srednja

Utjecaj: Visok

Ublažavanje:

- Strogo pridržavanje opsega Faze 0
- Zahtjevi za funkcionalnosti odgođeni za Fazu 1
- Tjedni pregledi napretka

### 8.2.2 Rizik: Zakašnjenja Projekta

**Vjerojatnost:** Srednja

**Utjecaj:** Srednji

**Ublažavanje:**

- Redovito praćenje prekretnica
- Rano identificiranje prepreka
- Fleksibilna alokacija resursa

## 9 Kriteriji Uspjeha

Faza 0 će se smatrati završenom kada:

1. Sve metode autentifikacije funkcionalne (Google OAuth, JWT, API ključevi)
2. Sve 3 osnovne uloge + 3 sposobnosti implementirane i testirane
3. Radni proces zahtjeva za sposobnosti funkcionalan za osnovne uloge i sposobnosti
4. Radni proces recenzije znanja operativan
5. Postojećih 1.300 PDF-ova migrirano s Day Zero pripisivanjem
6. Međukomponentna autentifikacija verificirana (KB ↔ MA)
7. Potpuno revizijsko bilježenje operativno
8. Sigurnosna revizija prošla
9. Korisnička dokumentacija potpuna
10. Administratorska dokumentacija potpuna
11. Svi jedinični, integracijski i E2E testovi prolaze
12. Sustav rukuje s 100+ istovremenih korisnika

## 10 Sljedeće Faze

Nakon uspješnog završetka Faze 0:

### 10.1 Faza 1: Stabilizacija Knowledge Buildera

- Ojačavanje CRUD operacija znanja s dozvolama
- Stabilizacija okvira agenata s pripisivanjem korisnika
- Dodavanje sveobuhvatne pokrivenosti testovima
- Implementacija CI/CD pipeline
- Optimizacija performansi

## 10.2 Faza 2: Prototip Modeling Assistanta

- Finaliziranje MA ugovora o integraciji znanja
- Implementacija izgradnje scenarija s dozvolama
- Kreiranje sučelja za sastavljanje modela
- Validacija end-to-end toka: znanje → modeliranje

## 10.3 Faza 3: Poboljšana Integracija i UX

- Napredno pretraživanje prilagođeno slučajevima modeliranja
- Vizualno istraživanje znanja u MA
- Značajke suradnje (dijeljeni scenariji)
- Praćenje doprinosa više korisnika

## 10.4 Faza 4: Proširenja i Dodaci

- Mehanizam dodataka za prilagođene alate
- Podrška za dodatne paradigme modeliranja
- Napredne značajke suradnje (radni prostori, timovi)
- Sustav povjerenja i reputacije

# 11 Zaključak

Faza 0 predstavlja kritičan temelj za AdvanDEB platformu, uspostavljajući sigurnost, kontrolu pristupa i infrastrukturu za suradnju. Pojednostavljena v3.0 arhitektura temeljena na sposobnostima pruža fleksibilnost uz smanjenje kompleksnosti u usporedbi s prethodnim dizajnim.

Po završetku, platforma će imati robustan, produkcijski spreman sustav autentifikacije koji se može skalirati za potporu budućim fazama.

Model temeljen na sposobnostima omogućuje korisnicima da povećavaju svoj pristup kako se njihove potrebe razvijaju, podržavajući cilj platforme poticanja suradnje uz održavanje kontrole kvalitete kroz radni proces recenzije.

**Verzija Dokumenta:** 3.0

**Datum:** 12. prosinca 2025.

**Status:** Spremno za Implementaciju

**Kontakt:** AdvanDEB Razvojni Tim