Çekmeköy Belediyesi Backend API

Mimari Yapılar ve Teknik Güçlü Yönler - A3 yatay görsel rapor

Anlık görüntü: 10.06.2026
Kaynağın tek doğru hâli backend kodudur

.NET 8 + ASP.NET Core | EF Core 8 + MSSQL | JWT çift kimlik sistemi | FluentValidation | Clean Architecture

1 Mimari temel

- Clean Architecture: Api / Core / Infrastructure; bağımlılıklar içe doğru, Core katmanı saf .NET.
- Repository + UnitOfWork: Generic Repository<T>, entity-specific repository ve WhereIf extension.
- Per-endpoint DTO tasarımı: her endpoint kendi Request/Response sözleşmesine sahip.
- Manuel mapping extension'ları: AutoMapper yok; derleme zamanı güvenliği ve runtime sürprizi yok.
- Standart response zarfı: BaseResponseModel<T> / PagedResponseModel<T>.
- Domain state machine: bilet/rezervasyon geçiş kuralları domain katmanında zorlanır.

2 Kimlik doğrulama & yetkilendirme

- Admin ve vatandaş JWT'leri ayrı secret ile imzalanır; token izolasyonu matematiksel olarak sağlanır.
- Zorunlu 2FA: admin ve vatandaşta şifre + SMS OTP; vatandaşta passwordless OTP de var.
- RBAC + granüler yetki kodları: rol bazlı atama ve kullanıcı bazlı allow-only override.
- Permission cache: etkin yetkiler 5 dk TTL ile IMemoryCache'te; değişimde cache invalidation.
- Refresh token rotasyonu: immutable token store ile audit izi korunur.
- NVİ/SAYSİS doğrulama ve X-Api-Key ile ayrı integration kimlik katmanı.

3 Güvenlik sertleştirmeleri

- Rate limiting: public-read 100/dk, public-write & sensitive 10/dk, admin 200/dk.
- Brute-force lockout: 5 başarısız giriş / 15 dk sonrası hesap 15 dk kilitlenir.
- İmzalı QR: HMAC-SHA256 ile sunucu imzalı bilet QR'ı.
- Server-generated 12 karakter base32 kodlar; tahmin edilemez bilet/kart kodları.
- PII masking: public response'larda ad, telefon ve TCKN maskelenir.
- Config-driven CORS, güçlü şifre yaşam döngüsü, WDAC + code signing.

4 Veri katmanı disiplinleri

- Soft delete + audit: fiziksel silme yok; tüm tablolarda oluşturma/güncelleme izi.
- Optimistic concurrency: kritik tablolarda RowVersion; çakışmalarda anlamlı 409.
- Order yönetimi: 26 entity'de tutarlı sıralama modeli ve scope bazlı unique index.
- Filtered unique index convention: unique index'ler otomatik WHERE IsDeleted=0.
- Transaction primitivi: çok-kayıtlı atomik işlemler ExecuteInTransactionAsync ile yönetilir.
- Deterministic seed + idempotent migration akışı: DEV/GGTECH senkron tutulur.

5 Entegrasyonlar & operasyon

- SMS gateway + OTP altyapısı: amaç bazlı 6 haneli OTP, 3 dk TTL ve rate limit koruması.
- Mock stratejisi: gerçek tablo + deterministic seed; API gelince sadece veri kaynağı değişir.
- Tutarlı Türkçe hata sözlüğü: kullanıcıya gösterilebilir, alan bazlı mesajlar.
- Turnike donanım entegrasyonu: geçiş kayıtları API üzerinden, sadakat kartı erişim kontrolü.
- FluentValidation: global filter ile otomatik tetiklenir, tüm mesajlar Türkçe.

Not: Üst metrik adetleri bu görsel versiyonda bilinçli olarak çıkarılmıştır; numaralandırma içerik bölümlerinden 1 ile başlar.

A3 yatay / 420 × 297 mm