Multi-Tenant-SaaS · Software-/Backend-Architektur

NestJS (Domain-Driven Design) · PostgreSQL Row-Level-Security · REST + WebSocket · BullMQ-Worker · Redis · JWT/2FA · anonymisiert

Clients
Web-SPA (TypeScript) · REST-/WebSocket-Consumer

API-/Edge-Schicht (NestJS)

REST-API
/api/v1 · versioniert

WebSocket-Gateway
Echtzeit-Events

Auth
JWT (15m/7d) · 2FA (TOTP) · API-Keys

Schutz
Rate-Limiting (Redis) · DTO-Validation

Application Layer — NestJS · Domain-Driven Design (Bounded Contexts)

Auth / Security
Application · Domain · Infrastructure
RBAC · 2FA · API-Keys · Audit

Mandanten-Verwaltung
Application · Domain · Infrastructure
Tenants · Rollen · Provisionierung

Kern-Domäne (Fach-Module)
Application · Domain · Infrastructure
Geschäftslogik · Workflows · Events

Abrechnung / Billing
Nutzung · Pläne · Limits

Benachrichtigung
E-Mail · WebSocket-Push · ntfy

Integration / API-Gateway
externe Dienste · Adapter (ACL)

Querschnitt: Guards (JWT/RBAC) · Interceptors · Validation-Pipes · Domain-Events (EventEmitter2, in-process) · Repository-Pattern (TypeORM)

Async-Verarbeitung
Queue: BullMQ → Worker
Background-Jobs · Retries
(RabbitMQ-/Broker-Pattern)
entkoppelt von Request-Pfad

PostgreSQL
Row-Level-Security · Multi-Tenancy
21 Schemas · UUID v7
AES-256-GCM (PII) + Blind-Index
eine DB · tenant_id-Isolation

Redis
Cache · Sessions
Pub/Sub · Rate-Limiting
TTL, kein PII im Klartext

HashiCorp Vault
Secrets-Management
per-Tenant Key-Derivation
HKDF · Crypto-Authority

★ Mandanten-Isolation (der Kern der Multi-Tenancy)

Jeder Request trägt eine tenant_id → PostgreSQL Row-Level-Security (FORCE) erzwingt Zeilen-Isolation pro Mandant — eine DB, harte Trennung.
PII pro Tenant AES-256-GCM verschlüsselt, Schlüssel via Vault (HKDF) abgeleitet. Domain-Schicht bleibt framework-frei (DDD), externe SDKs nur über Adapter (ACL).

Datenspeicher (PostgreSQL · Redis · Vault) · Client (Web-SPA / API-Consumer) · Edge/API + Datenbank · Application Layer (DDD) · Async (Queue/Worker)

anonymisiertes Architektur-Muster der eigenen Multi-Tenant-SaaS-Plattform — generische Bounded Contexts, keine Produkt-Internas. Stack 1:1 wie betrieben.

Stack: NestJS · PostgreSQL/RLS · Redis · BullMQ · WebSocket · JWT/2FA · TypeORM · DDD · anonymisiert