```
module: 27
title: Auth / Multi-Tenancy / Rollen / Permissions
phase: 1
status: detail-spec-draft
last_updated: 2026-05-08
session_source: brainstorming-session-2026-05-07-2206.md
related_lps: [LP-1, LP-2, LP-3, LP-6, LP-8, LP-9, LP-10]
spec_style: requirements-pur
```

Modul 27 — Auth / Multi-Tenancy / Rollen / Permissions

> ***Detail-Spec gemäß LP-9.*** *Plattform-Fundament. Alles andere baut darauf auf.*

Themenblöcke

```
A. Multi-Tenancy-Modell + URL-Struktur
B. Auth-Methoden
C. Rollen & Permissions
D. User-Lifecycle
E. API-Keys & technische Auth
F. Feature-Gating
```

Block A — Multi-Tenancy + URL-Struktur

A.1 — Tenant-Anlage

Zwei Pfade:

Pfad 1: Self-Service (`hivegrid.de` → Marketing-Site, externe Next.js-App, NICHT Teil der SaaS-Codebase). Signup-Form auf `hivegrid.de/signup` leitet zu `app.hivegrid.de/signup` zur Account-Erstellung.

Pfad 2: Enterprise (Demo-Buchung über externes Tool auf Marketing-Site, manuelle Tenant-Anlage durch Plattform-Admin nach Vertrag).

Self-Service-Signup-Formular:

Feld	Pflicht	Anmerkung
Email	✓	wird zum User-Account-Identifier
Passwort	✓	NIST-konform (siehe B.1)
Firmenname	✓	wird zum Default-Tenant-Slug
Vor-/Nachname	✓	
Branche	✓	SHK pre-selected, andere als „Coming soon" sichtbar
Größe	✓	Dropdown 1-10 / 11-25 / 26-50 / 51-100 / 100+ MA
AGB-Akzeptanz	✓	Checkbox
DSGVO-Akzeptanz	✓	Checkbox
AVV-Akzeptanz	✓	Checkbox (PDF wird elektronisch unterschrieben)
Telefonnummer	optional	für Support
USt-Id	optional	für Rechnungen

A.2 — Tenant-Slug

- **Auto-Generierung** aus Firmenname → `geerkens-gmbh` (lowercase, Bindestrich-getrennt, Umlaute → ae/oe/ue, Sonderzeichen weg, Suffix wie GmbH/AG/UG bleibt drin)
- **User darf editieren** im Signup-Formular
- **Live-Validierung** beim Tippen:
- Nur `[a-z0-9-]`, mind. 3, max. 40 Zeichen
- Reserved Words: `admin`, `app`, `api`, `www`, `help`, `support`, `marketing`, `dev`, `test`, `signup`, `login`, `auth`, `static`, `assets`, `public`, `settings`, `portal`, `buch`, `f`
- Eindeutigkeit live geprüft (debounced 500ms), bei Konflikt Vorschlag mit Nummer (`geerkens-gmbh-2`)
- **Slug ist nach Anlage NICHT änderbar** (Bookmark-Stabilität, Auth-URL-Stabilität). Migration-Tool ggf. später als Plattform-Admin-Funktion.

A.3 — URL-Struktur

```
hivegrid.de              → Marketing-Page (Next.js, extern)
app.hivegrid.de          → SaaS-Anwendung (Tenant-Welt)
admin.hivegrid.de        → Plattform-Admin (wir, Software-Betreiber)
```

Routen auf `app.hivegrid.de`:

```
/                                → Login (oder Tenant-Switcher wenn schon eingeloggt)
/signup                          → Self-Service-Signup
/login                           → Email/Passwort-Login
/forgot-password                 → Passwort-Reset
/verify-email                    → Email-Verification
/accept-invitation/{token}       → MA-Einladung annehmen

/{tenant}/                       → Tenant-Dashboard (Default nach Login)
/{tenant}/contacts               → CRM
/{tenant}/deals                  → Sales-Pipeline
/{tenant}/projects               → Auftragspipeline
/{tenant}/...                    → Modul-Routen

/{tenant}/settings/              → Persönliche Settings (jeder User)
/{tenant}/admin/                 → Workspace-Verwaltung (nur tenant.admin)

/portal/{tenant}/                → Customer-Portal (eigene User-Klasse)
/help/{lang}/{slug}              → Öffentliches Help-Center
/buch/{tenant}/{slug}            → Öffentliche Booking-Page
/f/{tenant}/{form-slug}          → Embedded-Form

/api/v1/...                      → Public REST-API
```

Trennung Tenant-Admin vs. Settings:
- `/settings/` = persönlich (Profil, Sprache, Theme, Notifications, 2FA, OAuth-Connects, Account löschen)
- `/admin/` = Workspace-Verwaltung (Mitarbeiter, Rollen, Groups, Billing, Integrationen, API-Keys, Branding (P2), Audit-Log, Export, Lösch-Workflow). Permission-gegated mit `tenant.admin`.

Multi-Tenant-Membership (Anforderungen):
- Default nach Login: letzter genutzter Tenant
- Benötigt: Tenant-Switcher-Komponente (überall in der App verfügbar) mit Liste aller Tenants des Users + Suchfeld-Funktion bei 5+ Tenants
- Erst-Login mit 2+ Tenants: separater Tenant-Auswahl-Screen
- `last_accessed_at` pro Tenant für Default-Sortierung

Custom-Domain: Phase 2, nur Enterprise (`crm.geerkens.de` als CNAME-Alternative zu `app.hivegrid.de/geerkens`).

A.4 — Datenisolation / RLS-Pattern (bauliche Vorgabe)

- Jede tenant-scoped Tabelle hat `tenant_id UUID NOT NULL`
- Policy SELECT/UPDATE/DELETE: `USING (tenant_id = current_setting('app.tenant_id')::uuid)`
- Policy INSERT: `WITH CHECK (tenant_id = current_setting('app.tenant_id')::uuid)`
- App-Role hat **kein** `BYPASSRLS`-Privileg
- Superuser-Role ausschließlich für Migrations
- Middleware setzt: `SET LOCAL app.tenant_id = '...'` pro Request
- Sonderfälle (kein RLS, App-Code permission-gegated): `users`, `subscription_plans`, `feature_flags`, `branchen_templates`
- Hintergrund-Jobs (Worker, Scheduler) setzen Tenant-Context explizit pro Job
- **Storage-Isolation:** Scaleway-Bucket-Pfad `tenants/{tenantId}/...`
- **Cache-Isolation:** Redis-Keys mit Präfix `tenant:{tenantId}:...`

A.5 — Tenant-Lifecycle

Status-Werte:

```
trial             → Self-Service-Tenant in Trial-Phase (5-7 Tage)
active            → Bezahlend
past_due          → Stripe-Zahlung gescheitert, Read-Only-Modus
frozen            → Tenant zahlt reduzierte Gebühr, Workspace read-only, jederzeit reaktivierbar
suspended         → Manuell gesperrt von Plattform-Admin (z.B. AGB-Verstoß)
deletion_pending  → Kündigung läuft, 30-Tage-Grace
deleted           → Hard-Delete erfolgt
```

Übergänge:
- `trial → active`: nach Zahlungs-Setup
- `active → past_due`: Stripe-Webhook bei Fehlversuch
- `past_due → active`: nach Nachzahlung
- `past_due → deletion_pending`: nach 30 Tagen Read-Only
- `active → frozen`: User klickt „Workspace pausieren" + reduzierten Plan bestätigen
- `frozen → active`: User klickt „Reaktivieren" + Standard-Plan
- `frozen → past_due`: bei Zahlungsausfall der reduzierten Gebühr
- `* → deletion_pending`: User klickt „Tenant kündigen"
- `deletion_pending → active`: User klickt „Kündigung zurückziehen" innerhalb 30 Tagen
- `deletion_pending → deleted`: nach 30 Tagen (Cron)
- `* → suspended`: Plattform-Admin
- `suspended → active`: Plattform-Admin

Frozen-Modus Rechte:

Aktion	Erlaubt
Login (alle Rollen)	✓
Daten lesen	✓
Schreibende Aktionen	✗
Email/WhatsApp/Push senden	✗
Automationen ausführen	✗
Eingehende Webhooks	✗ (verworfen, nicht gequeued)
Customer-Portal-Zugang (read-only)	✓
API (Read)	✓
API (Write)	✗

UI-Banner pro Status:
- `past_due`: *„Zahlung fehlgeschlagen, Konto in 14 Tagen gesperrt — [Klick hier]"*
- `frozen`: *„Workspace pausiert. Reaktivieren um wieder zu schreiben."*
- `deletion_pending`: *„Konto wird in X Tagen gelöscht — [Kündigung zurückziehen]"*
- `suspended`: Login-Page Klartext *„Konto temporär gesperrt — Support kontaktieren"*

Block B — Auth-Methoden

B.1 — Email + Passwort

Passwort-Anforderungen (NIST-konform):
- Mind. 12 Zeichen
- Keine erzwungenen Sonderzeichen-Regeln

- Check gegen **Have-I-Been-Pwned**-API (Top-1M-Liste lokal): Block bei Treffer mit Klartext: *„Dieses Passwort wurde in einem bekannten Datenleck gefunden — bitte ein anderes wählen."*
- Bcrypt mit Cost-Faktor 12

Login-Schutz:
- Rate-Limit pro Email: 5 Fehlversuche in 15 Min → 15 Min Lockout
- Rate-Limit pro IP: 50 Versuche/h
- Captcha (hCaptcha, DSGVO-konform) ab 3. Fehlversuch

Passwort-Reset:
- Magic-Link-Email mit 1h-Token, einmalig nutzbar
- Bei Reset: alle aktiven Sessions invalidiert

B.2 — Magic-Link (Login-Alternative)

- Token: 64 Zeichen, kryptographisch sicher, URL-safe
- Lebenszeit: 15 Minuten, einmalig nutzbar
- Rate-Limit: max. 3 Anfragen/Email/15min
- 2FA wird trotzdem abgefragt (Magic-Link ersetzt nur Passwort)
- Klartext-Hinweise für Token-abgelaufen / bereits-genutzt / Email-Verzögerung

B.3 — Microsoft-OAuth

→ **Backlog (Phase 2 oder später).** Nicht in Phase 1.

B.4 — 2FA (TOTP)

- **TOTP only** (Google Authenticator, Authy, 1Password, Bitwarden, etc.)
- **Keine SMS**
- Backup-Codes: 10 einmalige Recovery-Codes beim Aktivieren
- Setup-Flow: QR-Code + Secret in Klartext → Authenticator-App scannt → Test-Code → Backup-Codes-Download

Login-Flow mit 2FA:
- Nach Pwd/Magic-Link: 6-stelliger-Code-Eingabe
- Rate-Limit: max. 5 Versuche/5min

Trust-Device-Option:
- Checkbox: *„Auf diesem Gerät 30 Tage merken"*
- Signed Cookie umgeht 2FA für 30 Tage
- Trust-Device-Liste in `/settings/security/` mit individuellem Revoke

Recovery:
- Backup-Code → einmal-Login + Aufforderung neue 2FA einzurichten
- Backup-Codes weg → Tenant-Admin kann 2FA für User zurücksetzen (mit Audit-Log)
- User selbst Tenant-Admin und alleine → Plattform-Admin-Reset über Support

Pflicht-2FA:
- Default: Pflicht für `tenant.admin`-Permission, optional für Rest
- Tenant-Admin kann Toggle setzen: *„2FA für alle User dieses Tenants verpflichtend"* → User ohne 2FA werden beim nächsten Login zur Einrichtung gezwungen

B.5 — Session-Management

- **Server-Side-Sessions** in Postgres (nicht JWT — Logout/Revoke wäre mit JWT problematisch)
- HTTP-only, Secure, SameSite=Lax Cookie
- Default-Lebenszeit: 30 Tage Sliding-Window
- Tenant-Admin-konfigurierbar pro Tenant (max. Lebenszeit)
- Inaktivitäts-Timeout: 4h ohne Aktivität → Soft-Refresh + 2FA-Re-Verify falls aktiv

• Browser-Fingerprint (UA + IP-Range): bei deutlicher Abweichung → Re-Login

Session-Übersicht in `/settings/security/`:
- Liste aller aktiven Sessions: Gerät, Browser, IP, Letzte Aktivität, Standort (IP-Geolocation)
- Pro Session: Abmelden-Button
- Globaler „Von allen Geräten abmelden"-Button

Auto-Logout-Trigger:
- Passwort/2FA/Email geändert → alle Sessions weg
- User-Deaktivierung → alle Sessions weg
- Tenant-Suspended/Deleted → alle Sessions weg

Block C — Rollen & Permissions

C.1 — Permission-Modell: Variante 2 + Advanced

Default-View für Tenant-Admin im Rollen-Editor: Bundle-Stufen pro Modul.

```
crm.none          → kein Zugriff
crm.read_own      → eigene Kontakte/Deals sehen
crm.read_all      → alle sehen
crm.write         → eigene anlegen/bearbeiten
crm.admin         → Modul-Settings, Custom-Felder, alle löschen
```

Advanced-Mode: Toggle „Erweiterte Berechtigungen anzeigen" → klappt atomare Permissions auf. Bundle-Header zeigt *„Benutzerdefiniert"*, falls atomare Auswahl nicht zu Standard-Bundle passt.

Code-Internal: Permissions sind atomar gespeichert. Bundles sind Pre-Sets aus atomaren Permissions.

C.2 — 7 SHK-Template-Rollen (Seeding bei Tenant-Anlage mit Branche=SHK)

Rolle	Kern-Rechte	Tenant-Admin	UI-Modus Default
GF / Geschäftsführer	Alles, Tenant-Admin	✓	Büro
Vertriebsleiter	CRM admin, Sales-Pipeline admin, Lead-Inbox admin, Email-Marketing admin, Reports lesen. Projekte read_all.	✗	Büro
Vertriebler	CRM read_all + write_own, Pipeline read_all + write_own, Lead write, Booking write_own.	✗	Büro (mobil-fähig)
Projektleiter / Bauleiter	Projektpipeline admin (eigene), Plantafel write_own, Tasks write + assign, Files read_all + write, HR-Genehmigungen für eigene Monteure.	✗	Büro (mobil-fähig auf Baustelle)
Büro / Backoffice	CRM read_all, Pipeline read_all, Projektpipeline write, HR-Hub admin, Booking admin, Email-Inbox read_all, Files write.	✗	Büro
Marketing	CRM read_all + Segmente, Email-Marketing admin, Form-Builder admin, Lead-Inbox write, Booking read. Kein HR/Projekt-Edit.	✗	Büro
Monteur	Projektpipeline read_own + nur aktive, Tasks own + edit, Acceptance write, Foto-Forms write, Files read in Projekt + write Fotos, Chat in eigenen Projekt-Channels, HR-Hub read_own. Kein Sales/Marketing/Admin.	✗	**Baustelle**

Sonderpunkte:
- **UI-Modus** (LP-2): Default je nach Rolle, **vom User pro Gerät überschreibbar** (Vertriebler kann auf iPhone auf „Baustelle" umschalten)
- **Tenant-Admin** in Phase 1 nur GF (Custom-Rollen können das später erweitern)
- **Endkunde** ist *keine* Tenant-Rolle (eigene `PortalUser`-Klasse, Modul 15)

Wichtige Architektur-Vorschrift: Diese 7 Rollen sind **nicht hartkodiert**, sondern **deklaratives SHK-Branchen-Template**. Beim Tenant-Anlegen mit Branche=SHK wird das Template geseeded. Andere Branchen haben eigene Default-Rollen-Templates. Tenant-Admin kann nach Anlage **alle** Rollen vollständig editieren/umbenennen/löschen/neue anlegen.

C.3 — Custom-Rollen + Edit-Logik

Editor unter `/{tenant}/admin/roles/`:

- Liste aller Rollen mit User-Anzahl pro Rolle
- **Neue Rolle anlegen** (komplett von Null möglich, oder „Basieren auf"-Dropdown als Ausgangspunkt — kopiert Permissions als Snapshot)
- Editieren: Name, Beschreibung, Permissions, Default-UI-Modus
- Duplizieren mit Suffix „(Kopie)"
- Löschen: Block falls noch User zugewiesen → Ersatz-Rolle wählen oder Bulk-Reassign

Standard- vs. Custom-Rollen: Alle Rollen nach Anlage **vollständig editierbar**. Internes Flag `is_template_origin: true/false` nur als Hinweis, keine Funktions-Einschränkung.

Inheritance: Keine Live-Inheritance. Permissions werden beim Anlegen kopiert (Snapshot).

Multi-Rolle pro User: möglich. Permissions additiv kombiniert. Bei UI-Modus-Konflikt → umfangreichere UI als Default.

Default-Rolle bei neuen Usern: Tenant-Admin wählt beim Einladen explizit, kein globales Default.

Klartext-Fehler:
- Permission-Konflikte: *„Diese Permission-Kombination ist inkonsistent (z.B. ‚Deals löschen' aber kein ‚Deals lesen'). Wir aktivieren ‚Deals lesen' automatisch dazu."*
- Last-Tenant-Admin-Rolle löschen: Block + Klartext

C.4 — Groups

Orthogonal zu Rollen — keine Permission-Wirkung.

Use-Cases (Geerkens): „Team Süd"/„Team Nord", „Außendienst"/„Innendienst", „Praktikanten"/„Festangestellte".

Spec:
- User in mehreren Groups möglich
- Genutzt für: Filter in Listen, Mass-Assign (Files/Projekte), Notifications, Automation-Bedingungen
- Editor unter `/{tenant}/admin/groups/`: Liste mit Mitgliederzahl, anlegen/umbenennen/löschen, Bulk-Add/Remove, Description
- Keine Hierarchien in Phase 1
- Klartext bei Lösch mit Mitgliedern: *„Diese Group hat 8 Mitglieder. Bei Löschen verlieren sie die Zuordnung."*

C.5 — Permission-Audit & Edge-Cases

- **Audit-Trail:** jede Rollen-/Permission-Änderung mit Diff geloggt
- **Permission-Preview-Tool** in `/admin/users/{id}/`: zeigt aufgelöste effektive Permissions mit Quellen-Hinweis
- **Self-Permission-Schutz:** Tenant-Admin kann sich nicht selbst die Permission entziehen, wenn er einziger ist
- **Group-Mitgliedschaft:** vergibt KEINE Permissions in Phase 1
- **Concurrent-Update:** Last-Write-Wins mit Klartext-Konflikt-Hinweis bei Mehrfach-Edit

---

Block D — User-Lifecycle

D.1 — User-Einladung

Flow: Tenant-Admin in `/admin/users/` → „Mitarbeiter einladen" → Modal (Email Pflicht, Name optional, Rolle Pflicht, Groups optional, Persönliche Nachricht optional) → System legt `TenantUserInvitation` an mit 7-Tage-Token → Email mit Magic-Link.

Drei Pfade beim Klick:
- **(a) Email noch nicht im System:** Account-Erstellung (Pwd, ggf. 2FA-Setup) → Tenant-Onboarding-Wizard
- **(b) Email im System (anderer Tenant):** Login → automatisch Mitglied → Welcome-Hinweis im Switcher
- **(c) Email bereits Mitglied dieses Tenants:** Klartext-Fehler beim Einladen schon: *„Max Mustermann ist bereits Mitglied — Rolle: Vertriebler"*

Edge-Cases:
- Token-Lebensdauer 7 Tage; bei Ablauf „Erneut senden"
- Max. 3 aktive Einladungen pro Email pro Tenant
- Bulk-CSV-Invite: **Phase 2**

D.2 — Deaktivierung & Entfernen

Modus 1 — Deaktivieren (vorübergehend):
- TenantUser bleibt, Status=`disabled`
- Sessions invalidiert, kein Login mehr möglich
- Re-Aktivierung jederzeit ohne neue Einladung

Modus 2 — Aus Workspace entfernen (permanent):
- TenantUser-Beziehung gelöscht
- 2FA-Trust-Devices invalidiert
- Audit-Trail bleibt, User wird als „ehemaliger Mitarbeiter" angezeigt
- Re-Aufnahme nur durch neue Einladung

Vor beiden Modi: Reassign-Workflow

Wenn der zu deaktivierende User noch zugewiesene Entitäten hat, wird ein Bestätigungs-Workflow erzwungen, bevor die Deaktivierung greift. Folgende UI-Elemente werden benötigt:

- Anzeige aller offenen Verknüpfungen pro Typ (Deals, Projekte, Tasks, Termine, ...) mit Anzahl
- Bulk-Reassign-Funktion (alle Verknüpfungen an eine Person/Group)
- Einzel-Reassign-Funktion (pro Entität individuell)
- Override-Bestätigungs-Funktion *„Ohne Zuweisung lassen — Daten bleiben verwaist"* (nicht empfohlen, mit explizitem Bestätigungs-Schritt)

Klartext-Fehler:
- Last-Tenant-Admin entfernen: Block
- Sich selbst entfernen: Block, Klartext: *„Du kannst dich nicht selbst entfernen. Bitte einen anderen Tenant-Admin oder kündige deinen Account in den Settings."*

D.3 — Account-Löschung (Apple-Pflicht + DSGVO)

Multi-Step-Bestätigung in `/{tenant}/settings/account/`:

- **Step 1 — Erklärung:** Klartext was gelöscht / was anonymisiert / was bleibt
- **Step 2 — Identität:** Pwd oder Magic-Link + 2FA falls aktiv
- **Step 3 — Edge-Cases:** falls einziger Tenant-Admin in mind. 1 Tenant → Block mit Klartext + Direkt-Link zum Lösen
- **Step 4 — Final-Klick** mit 3-Sek-Countdown auf Button

Was technisch passiert:
- TenantUser-Beziehungen gelöscht
- PII-Felder mit `[deleted-{userId}]` überschrieben (FKs intakt)
- Audit-Spuren behalten User-ID, zeigen „ehemaliger Mitarbeiter"
- 2FA-Geräte/Sessions/Push-Tokens entfernt
- Verbundene OAuth-Konten getrennt
- Avatar-Datei aus Storage gelöscht

Bestätigungs-Email + 24h-Reverse-Window:
- Email an Lösch-Adresse: *„Dein Account wurde gelöscht am [Datum]. Falls nicht von dir, kontaktiere uns innerhalb 24h: [Support-Link]"*
- Support kann innerhalb 24h wiederherstellen (mit Audit-Eintrag)

D.4 — Multi-Tenant-Membership & Tenant-Wechsel

- **Erst-Login mit 1 Tenant:** automatisch ins Dashboard
- **Erst-Login mit 2+ Tenants:** separater Tenant-Auswahl-Screen
- **Folge-Logins:** letzter genutzter Tenant (siehe `last_accessed_at`)
- **Tenant-Switcher-Komponente** muss überall in der App verfügbar sein, mit Liste aller Tenants des Users + Suchfeld bei 5+ Tenants
- **Tenant verlassen** in `/settings/account/`: Multi-Step + Reassign-Workflow + Last-Tenant-Admin-Schutz
- **User landet ohne Tenant:** Klartext-Screen mit Funktionen *„Neuen Workspace anlegen"* und *„Auf Einladung warten"*
- `last_accessed_at` pro Tenant für Default-Sortierung

Block E — API-Keys

Verwaltung in `/{tenant}/admin/api-keys/`:

- Liste: Name, Scopes, Erstellt-Datum, Letzte Nutzung, Status
- Anlage: Name + Scopes → Key einmalig sichtbar (Copy-to-Clipboard mit Klartext-Warnung)
- Widerrufen mit einem Klick
- Detail-View: Logs der letzten 100 Anfragen (Endpoint, Status, Antwort-Zeit, IP)

Authentifizierung:
- `Authorization: Bearer <key>` Header
- Query-Param `?api_key=...` nur für GET-Webhook-Inbound mit Klartext-Warnung im UI

Scopes (Variante-2-Bundles):
- `read_only` — alle GET-Endpoints (Default)
- `webhook_inbound` — nur eingehende Lead/Form-Webhooks
- `read_full` — alle GET inkl. sensible Daten (Mails, HR)
- `automation_trigger` — kann Trigger in Engine auslösen

Rate-Limiting: 1.000 Req/h Default, Tenant-Admin kann erhöhen, 429 mit Klartext-Body.

Sicherheits-Defaults:
- 365-Tage-Ablauf (erzwingt Rotation)
- Keys gehören dem Tenant, nicht dem User (überleben User-Deaktivierung)
- Audit-Log pro Anlage / Widerruf / Fehlernutzung

Phase 2: OAuth2-Provider-Modus, granulare Scopes, API-Versioning.

Block F — Feature-Gating

F.1 — Subscription-Feature-Gates

Datenmodell (Modul 28):

```
SubscriptionProduct (z.B. "Cloud", "Cloud+", "Enterprise")
  ├── enthält viele SubscriptionFeatures (z.B. "crm", "automation", "kwp_integration")
  └── verknüpft mit Stripe-Price
TenantSubscription
  └── verweist auf SubscriptionProduct + Status
```

Code-Convention (Loader-First-Call):

```
await requireTenantFeatureAccess(tenantId, 'kwp_integration')
```

Bei kein Zugang → Loader wirft → React-Boundary zeigt Klartext: *„Die KWP-Integration ist im Cloud-Plus-Plan verfügbar. Mehr erfahren auf hivegrid.de/pricing"* → Link führt **außerhalb der App** zur Marketing-Site (Apple-Compliance).

Gate-Granularität:
- Pro Modul auf Tenant-Ebene
- Pro Feature innerhalb Modul wenn nötig (z.B. `automation.advanced_branches`)

Pricing-Definitionen geparkt — Engine baut bereits, konkrete Plans später definiert.

F.2 — Feature-Flags (Modul 32)

- Boolean pro Tenant von uns Admin-side aktivierbar (`admin.hivegrid.de/feature-flags`)
- Code: `if (await tenantHasFlag(tenantId, 'beta_new_dashboard')) { ... }`
- Default-Wert pro Flag
- Filter (z.B. „Tenants > 50 MA")
- Audit-Log bei Flag-Änderung

Flag-Lifecycle:
- `beta` → einzeln aktiviert für Test-Tenants
- `rollout` → breit aktiviert über Filter
- `GA` → Flag aus Code entfernt (always-on)
- `deprecated` → Default false, Code wird entfernt

Klartext: Tenants sehen kein UI für Flags — Features einfach sichtbar/nicht. Phase 2: Tenant-self-service-Flags.

Architektur-Vorschriften (Querschnitt)

Bezug aus Master-Session-Datei (Architektur-Vorschriften):
- LP-3, AV #3 — **Branchen-Templates deklarativ:** SHK-Rollen sind Seeding, nicht Hardcode
- LP-10, AV #1 — **Klartext-Diagnostik:** alle Auth/Permission-Fehler mit menschenlesbarem Text + Lösungs-Hinweis
- AV #5 — **Permissions-aware-Default:** alle Listen/Suchen filtern automatisch nach User-Permissions
- AV #6 — **Audit-Trail-Default:** alle schreibenden Aktionen geloggt
- AV #20 — **Action-Boundary für KI:** KI darf keine Permissions-Änderungen direkt durchführen, nur User-Bestätigt

---

Detail-Spec-Status: DRAFT

Erste vollständige Detail-Spec für Modul 27. **Vor Bau:** Verifizierung mit Noah (zusammen mit Pflichtenheft-Sweep). Bei Implementierung dann konkrete Permission-IDs, RLS-Policy-SQL, Stripe-Price-IDs ergänzen.

Offene Detail-Punkte (nicht-blockierend, beim Bau zu klären):
- Konkrete Permission-IDs pro Modul (entstehen modulweise mit den jeweiligen Detail-Specs)
- Konkrete UI-Layouts (Subframe-Designs kommen separat)
- Migrations-Skripte / Seeding-SQL (Implementierungs-Detail)