AUDIT-11 — Belege

Stand: 2026-05-18

Code-Inspektion (Stand commit a1912073)

Datei	Zeile	Beleg-Typ
`ce-doc-portal/backend/api.py`	423–446	V1-Bug: vorgang_detail ohne Tenant-Check
`ce-doc-portal/backend/api.py`	541–558	V4-Bug: vorgang_akte_html ohne Tenant-Check
`ce-doc-portal/backend/api.py`	932–965	V5-Bug: OPL-POST ohne Tenant-Check
`ce-doc-portal/backend/api.py`	1050–1086	V2-OK: Mandanten-Endpoint mit Tenant-Anker
`ce-doc-portal/backend/auth_service.py`	79–105	V10: HMAC-Token mit Rolle, ohne berater_id-Claim
`core/skills/cdp/mandanten_db.py`	35–47	Verzeichnis-Trennung pro Koordinator (✓)

Verzeichnis-Belege

```
workspaces/
├── berater_demo/mandanten/...   # Tenant-Trennung Mandanten-Stammdaten ✓
├── berater_<id>/mandanten/...   # dito pro Koordinator
└── projects/                    # KEINE Tenant-Trennung — alle case_ids gleichberechtigt ✗
    ├── demo_knorre_cnc500/
    ├── demo_bauer_hyp3t_final/
    └── ...
```

→ Das Workspace-Layout selbst trennt Mandanten-Stammdaten korrekt, aber **Vorgänge liegen flach in `projects/`**. Der Bug ist also nicht im Verzeichnis-Layout, sondern im Endpoint-Check.

Stichproben

Stichprobe	Ergebnis
`state["meta"]["berater_id"]` in synth-Workspaces gesetzt?	Stichprobe `synth_cobot_vision_01/analyst_outputs/akt_state.json` enthält i. d. R. `meta.berater_id` → der Anker für den Fix existiert bereits
Default-Wert bei fehlendem berater_id	`api.py` Z. 271: Default `"demo"` → für Pilot-Mandanten muss berater_id zwingend gesetzt sein
`liste_mandanten` für Koordinator	Tenant-isoliert (✓) — Koordinator A sieht nur `workspaces/berater_A/mandanten/*`

Konkretes Reproduktions-Szenario (für Coaching-Audit-Demo)

1. Koordinator A loggt sich ins Portal ein
2. Koordinator A kennt aus einem öffentlichen Reifegrad-Beispiel die case_id `demo_knorre_cnc500`
3. Koordinator A ruft direkt `https://portal.ce-doc.eu/api/vorgang/demo_knorre_cnc500` auf
4. **Aktuell:** HTTP 200 mit vollem State des Knorre-Mandats
5. **Nach Fix:** HTTP 404 mit Log-Eintrag „cross-tenant-Zugriffs-Versuch"

Bezugsnormen — Anwendung im Audit

Norm	Klausel	Status
ISO 27001 A.9.4.1	„Information access restriction"	◐ — Bug in api.py
ISO 27001 A.9.4.4	„Use of privileged utility programs"	✓ — Bastion-only
OWASP ASVS V8.2.1	„Verify the application enforces access control"	✗ — Befund V1/V4/V5
OWASP ASVS V8.3.4	„Verify least privilege"	✓ — Rollen-Hierarchie funktioniert
BSI C5 BEI-04	„Trennung der Mandanten"	◐ — Mandanten ✓, Vorgänge ✗

Verifikation der Mitigation (post-Fix)

Wird im Folge-Lauf nach Schließung von AUDIT-11-F-01 erbracht: - Pytest-Test `test_tenant_isolation.py` mit allen 10 Vektoren - Integration in CI-Gate (PROC-K2) - Halbjährliches Re-Audit