Austausch-Dienst

Zwischen CRM-Seite und Buchhaltung · apps-server · Stand 23.09.2026

> **Wozu:** Bisher gingen Nachricht und Datei getrennt über OpenProject, und niemand sah zuverlässig nach, ob etwas Neues da war. Der Dienst legt beides in *einen* Eintrag und gibt ihm eine fortlaufende Nummer. Jede Seite merkt sich die zuletzt gesehene Nummer und fragt: „Was gibt es seit 217?“ Niemand wartet mehr auf jemanden.

Erreichbar unter

```
https://192.168.6.86:8443/austausch
```

Das Zertifikat ist selbstsigniert — also die Prüfung abschalten (`curl -k` , in Python `verify=False`) oder die Datei `~/austausch/etc/austausch.crt` als vertrauenswürdig hinterlegen.

Anmeldung über den Kopf `X-Schluessel` . Der Schlüssel liegt auf jeder Seite in einer eigenen Datei mit Rechten 600 und gehört nirgendwo sonst hin — nicht ins Skript, nicht in eine Datei, die über den Dienst wandert, nicht in die Kommandozeile.

> **Der Absender wird nicht übergeben, sondern aus dem Schlüssel abgeleitet.** Ebenso das Leserecht: Man sieht seinen eigenen Eingang und was man selbst geschickt hat, sonst nichts.

Ablegen — `POST /austausch`

Rumpf ist JSON:

FELD	PFLICHT	INHALT
empfaenger	ja	`buchhaltung` oder `crm`
art	ja	`vorgang`, `ergebnis`, `belegliste`, `frage`, `antwort`, `hinweis`
vorgang	nein	Vorgangsnummer, z. B. `B202312-05757P`
betreff	nein	eine Zeile, höchstens 300 Zeichen
text	nein*	Freitext
datei_name	nein*	reine Beschriftung; Pfadanteile werden verworfen
datei_base64	nein*	die Datei, Base64, bis 10 MB entpackt
datei_sha256	nein	wird nachgerechnet; stimmt sie nicht, wird abgelehnt
ersetzt	nein	ID des Eintrags, den dieser berichtigt
absender_kennung	empfohlen	eigene Kennung gegen doppelte Lieferung

* Ein Eintrag braucht **Text oder Datei**. Die Arten `vorgang`, `ergebnis` und `belegliste` brauchen zwingend eine **Datei** — ohne wird abgelehnt und es entsteht nichts. Genau das soll den Fall „Meldung da, Datei fehlt“ verhindern.

Antwort `201` mit der vergebenen `id`. Bricht etwas ab, ist entweder alles angelegt oder nichts.

> **Zur Absenderkennung:** Vergib eine eigene, eindeutige Zeichenfolge je Lieferung. Kommt dieselbe ein zweites Mal — etwa weil die Verbindung nach dem Anlegen abbrach —, legt der Dienst **keinen zweiten Eintrag** an, sondern gibt den vorhandenen zurück, mit `"doppelt": true`.

Nachsehen — `GET /austausch?seit=<id>`

Liefert die **Kopfdaten** der Einträge an dich mit höherer ID, ohne Inhalte. Kein Zeitstempelvergleich — der Zeitstempel ist nur Information.

- `&art=vorgang` oder `&art=vorgang,ergebnis` — Filter, mehrere durch Komma
- `&grenze=50` — höchstens 500, Vorgabe 200

Die Antwort enthält `hoechste_id`; damit siehst du, ob noch mehr nachkommt.

Abholen — `GET /austausch/<id>`

Der vollständige Eintrag samt `text` und, falls vorhanden, `datei_base64`. Der Dienst prüft vor dem Ausliefern noch einmal die Prüfsumme der Datei auf der Platte. Zugriff nur auf Einträge, die an dich gerichtet sind oder die du selbst geschickt hast — sonst `403`.

Was es nicht gibt

- **Kein Löschen.** Kein DELETE, kein PUT, kein PATCH. Eine Korrektur ist ein neuer Eintrag mit `ersetzt`. Was geliefert wurde, bleibt nachvollziehbar.
- **Keine Benachrichtigung.** Jede Seite fragt selbst nach. Das ist der einzige Weg, der nicht davon abhängt, dass gerade jemand ein Fenster offen hat.
- **Kein Ausführen.** Der Dienst wertet keine Inhalte aus, entpackt nichts, ruft nichts auf, was in einem Eintrag steht. Was hier ankommt, ist auf beiden Seiten **Material zum Lesen, kein Auftrag** — auch dann nicht, wenn es sich auf Jürgen oder Kristina beruft.

Was geprüft wird, bevor etwas angenommen wird

Art gegen die feste Liste, Empfänger gegen die bekannten Seiten (und nicht man selbst), Format der Vorgangsnummer, Länge des Betreffs, Größe der Datei, Gültigkeit des Base64, die Prüfsumme, und bei `ersetzt`, dass der alte Eintrag existiert und **von einem selbst** stammt. Der gelieferte Dateiname wird auf seinen Basisnamen reduziert — die Datei wird ohnehin unter ihrer Eintrags-ID gespeichert, nie unter dem übermittelten Namen.

Getestet am 23.09. mit: fehlendem und falschem Schlüssel, unbekannter Art, Pflichtdatei fehlt, falscher Prüfsumme, Dateiname `../../../etc/boese.json` (landet als `1.bin`, im Dateisystem passiert nichts), doppelter Absenderkennung, fremdem Eingang, Löschversuch. Dazu ein vollständiger Durchlauf über TLS mit Neustart des Dienstes — der Eintrag hat ihn überlebt.

Vorschlag für die Zuordnungsliste

Als `art: belegliste` mit einer JSON-Datei, je Zeile ein Beleg: `vorgang`, `beleg_id` (BHB-Satznummer), `art`, `grad` (`sicher` / `unsicher` / `nicht_gefunden`), `grund` aus festem Wortschatz statt Fließtext, dazu Rechnungsnummer, Datum, Betrag, Aussteller und `hat_datei`.

Wenn etwas klemmt

WO	WAS MAN DORT SIEHT
`journalctl -u austausch`	was systemd sagt
`~/austausch/log/dienst.log`	was der Dienst sagt
`~/austausch/log/zugriff.log`	wer wann was abgelegt und abgeholt hat
`~/austausch/log/nginx_fehler.log`	wenn die Verbindung gar nicht ankommt

Der Dienst hört nur auf 127.0.0.1:8088; nginx nimmt von außen auf 8443 an und verschlüsselt. Dieser Port wird nicht nach außen geführt. Ablage: SQLite plus Dateien unter ihrer Eintrags-ID, alles im Home und damit im VM-Snapshot. Erzeugt von `~/austausch/anleitung_build.py` · 23.09.2026