Technik und Sicherheit der docMan Box.

Für Interessenten und ihre IT-Betreuung · Stand 15.11.2026

docMan ist eine Software für Belege, Ablage und Buchhaltungsvorbereitung. In der Regel läuft sie beim Kunden auf einem eigenen kleinen Server im Büro (der „docMan Box“) – die Dokumente bleiben im Haus. Welche anderen Möglichkeiten es gibt, bis hin zur Cloud, steht in „Wo docMan läuft – die Möglichkeiten“. **Teil A** beschreibt, wie die Box eingerichtet und abgesichert ist und was wir bewusst **nicht** tun. **Teil B** beschreibt, welche Hardware und welches Umfeld wir voraussetzen, wenn der Kunde den Server selbst bereitstellt, und wie die Übergabe abläuft.

Kurz gesagt

- Die Daten liegen auf zwei gespiegelten SSDs, vollständig verschlüsselt (LUKS2, AES-256). Ohne das Gerät selbst sind sie nicht lesbar.
- Aus dem Büro-Netz ist nur docMan im Browser erreichbar (HTTPS, Port 443). Es gibt keine Portfreigabe am Router.
- Wir warten die Box ausschließlich über ein verschlüsseltes Tailscale-Netz, nur mit Schlüssel, nie mit Passwort.
- Die Box kann von sich aus **kein** anderes Gerät erreichen, weder im Kunden-Netz über unseren Zugang noch bei uns. Tunnel und Weiterleitungen sind abgeschaltet.
- Auf der Box laufen keine Remote-Editoren oder KI-Assistenten. Das ist technisch gesperrt.

Teil A – So ist eine docMan Box eingerichtet

Beschrieben an unserem Referenzgerät; jede Box wird gleich eingerichtet.

A1 · Hardware und System

Bestandteil	Ausführung
Gerät	Lenovo ThinkCentre M90q Gen 6 (Tiny), Intel Core Ultra 7 265, 32 GB RAM, ohne Windows
System-SSD	512 GB NVMe – nur Betriebssystem und Programme, keine Kundendaten
Daten-SSDs	2 × Samsung 990 Pro 2 TB NVMe als Spiegel (RAID 1)
Betriebssystem	Ubuntu Server 26.04.1 LTS (Langzeitpflege), minimal installiert, keine grafische Oberfläche
Firmware	UEFI mit Secure Boot an, TPM 2.0 an; nach Stromausfall startet das Gerät von selbst
Strom	USV APC Back-UPS BX750MI, fährt die Box bei Stromausfall sauber herunter

A2 · Speicher: Spiegel und Verschlüsselung

Die Kundendaten (Dokumente, Datenbank, Sicherungen) liegen ausschließlich auf dem verschlüsselten Spiegel:

```
2 × NVMe-SSD → RAID 1 (mdadm) → LUKS2-Verschlüsselung → ext4 → /srv/docman
```

- **Spiegel (RAID 1):** Beide SSDs enthalten jederzeit dasselbe. Fällt eine aus, arbeitet docMan ohne Unterbrechung auf der anderen weiter. Eine Bitmap sorgt dafür, dass nach Stromausfall oder Tausch nur geänderte Bereiche abgeglichen werden.
- **Verschlüsselung:** LUKS2 mit AES-XTS (256 Bit). Werden SSDs oder das ganze Gerät entwendet, sind die Daten ohne Schlüssel wertlos.

- **Entsperren ohne Passwort:** Den Schlüssel hält der Sicherheitschip (TPM 2.0) des Geräts. Er gibt ihn nur heraus, wenn das Gerät mit unveränderter Secure-Boot-Kette startet (PCR 7). Wird das Gerät von einem fremden Datenträger gestartet oder werden die SSDs in einen anderen Rechner eingebaut, bleiben die Daten verschlossen.
- **Notfallschlüssel:** Ein zweiter, langer Wiederherstellungsschlüssel existiert für den Fall eines Mainboard-Tauschs. Er wurde auf dem Gerät erzeugt, liegt nur im Passwortmanager des Kunden und wurde nie per Mail, Chat oder Datei weitergegeben.
- **System-SSD unverschlüsselt:** Bewusst, damit die Box nach Stromausfall ohne Eingabe startet. Dort liegen nur Betriebssystem und Programme. Auch die Datenbank liegt auf dem verschlüsselten Spiegel, nicht auf der System-SSD.

A3 · Netzwerk und Zugriff

Weg	Wer / was	Regel
Browser im Büro-LAN → Box	Mitarbeiter	Nur HTTPS (Port 443) auf docMan, Anmeldung mit Benutzer und Kennwort; Geräte außerhalb bekommen zusätzlich einen Code per Mail
Wartung (SSH) → Box	docMan (wir)	Nur über Tailscale (WireGuard-verschlüsselt), nur mit SSH-Schlüssel; aus dem LAN ist SSH gesperrt
Internet → Box	niemand	Keine Portfreigabe am Router nötig oder erwünscht; alle anderen eingehenden Verbindungen werden verworfen (Firewall ufw)
Box → Internet	Box	Ausgehend: Updates, Tailscale, Mail, das Einlesen von Dokumenten (siehe A6), die nächtliche Sicherung
Box → andere Geräte im Tailscale-Netz	Box	Gesperrt per Zugriffsregel (ACL): Die Box darf niemanden erreichen, nur wir dürfen zu ihr

SSH ist streng eingestellt: Anmeldung nur mit Schlüssel (Passwort- und Tastatur-Anmeldung aus), kein direkter root-Zugang, keine Weiterleitungen (TCP, Agent, Unix-Sockets, Tunnel und **X11** – alle aus). Damit kann über unseren Zugang kein Tunnel in das Kunden-Netz gebaut werden.

Keine Remote-Editoren: Werkzeuge wie VS Code Remote, Cursor oder Windsurf, die sich auf Servern einnisten und oft KI-Assistenten mitbringen, sind auf der Box gesperrt: Ihre Installationsordner sind durch leere, schreibgeschützte Dateien von root belegt, und ohne Weiterleitung könnten sie ohnehin nicht arbeiten.

Lauschende Dienste: Neben SSH und später docMan (443) lauschen nur Tailscale selbst und der lokale DNS-Dienst (nur innerhalb der Box). Jeder weitere Dienst ist bewusst nicht installiert.

A4 · Betrieb und Wartung

- **Sicherheitsupdates** spielt die Box täglich selbst ein (unattended-upgrades).
- **SSD-Zustand** (S.M.A.R.T.: Temperatur, Verschleiß, Fehler) und **Spiegel-Zustand** prüfen wir regelmäßig; eine Warnung geht an uns, bevor aus einem Verschleiß ein Ausfall wird.
- **Monatliche Spiegel-Prüfung** (Zeitplan des Systems, erster Sonntag im Monat): Beide SSDs werden vollständig gegeneinander gelesen und verglichen.
- **Unser Zugriff** dient Updates von docMan, der Kontrolle von Spiegel, SSDs und Sicherung und der Fehlersuche. In Dokumente schauen wir nur, wenn der Kunde für eine Fehlersuche darum bittet.

A5 · Sicherung

Jede Nacht entsteht eine verschlüsselte Sicherung von Datenbank und Dokumenten. Sie geht über Tailscale an einen Sicherungsort außer Haus und wird dort nur angehängt (append-only): Auch wer die Box übernimmt, kann alte Sicherungen weder ändern noch löschen. Den Schlüssel zum Öffnen der Sicherung hat die Box nicht – sie kann nur verschlüsseln. Wo die Sicherung liegt – bei uns, beim Inhaber zu Hause oder in einem deutschen Rechenzentrum –, hängt von der gewählten Möglichkeit ab; lesen kann sie dort niemand.

A6 · Was die Box nach außen gibt

docMan liest Belege mit einer KI (Claude von Anthropic) aus: Rechnungsnummer, Betrag, Lieferant, Kategorie. Dafür wird der Inhalt des jeweiligen Dokuments verschlüsselt an die Schnittstelle von Anthropic übertragen. Die Verarbeitung durch Anthropic erfolgt auf Grundlage des Data Processing Addendum (DPA) von Anthropic. Ein Auftragsverarbeitungsvertrag (AVV) zwischen Kunde und docMan regelt unseren Wartungszugriff und nennt die Unterauftragsverarbeiter (Anthropic, Sicherungsserver). Darüber hinaus verlässt nichts die Box außer Mails, die docMan im Auftrag des Kunden verschickt, und der verschlüsselten Sicherung.

A7 · Was wir vor jeder Übergabe prüfen

Prüfung	Wie
SSH nur mit Schlüssel	Passwort-Anmeldung versucht → abgewiesen
SSH-Weiterleitungen	alle aus, einschließlich X11
Abschottung	Box erreicht im Tailscale-Netz nichts; SSH aus dem LAN gesperrt
Neustart	Spiegel wird ohne Eingabe per TPM entsperrt
Stromausfall	Stecker gezogen → Box startet von selbst, Daten vollständig
SSD-Ausfall	eine SSD aus dem Spiegel genommen → Daten weiter les- und schreibbar, danach wieder vollständig
Notfallschlüssel	erzeugt und geprüft, liegt nur beim Kunden
Spiegel-Prüfung	beide SSDs vollständig verglichen
USV	Strom weg → sauberes Herunterfahren, Wiederanlauf
Sicherung	Sicherung und Wiederherstellung auf leeren Platz
Warnung bei SSD-Ausfall	Meldung in docMan und an uns
Rechte eingeschränkt	Wartungsbenutzer ohne pauschale Administratorrechte

Teil B – Wenn der Kunde den Server selbst stellt

Wir sind Softwareentwickler, keine Hardwarehändler, und verkaufen keine Geräte. Der Kunde kauft unser Referenzgerät selbst – oder er oder seine IT stellt einen anderen passenden Rechner bereit. Wir prüfen ihn aus der Ferne gegen diese Vorgabe und installieren docMan erst, wenn alles passt. Die Einrichtung ist danach dieselbe wie in Teil A.

B1 · Hardware

Bestandteil	Mindestens	Empfohlen
Bauform	Rechner für Dauerbetrieb, x86-64	Business-Mini-PC (z. B. Lenovo ThinkCentre Tiny, HP Elite Mini, Dell OptiPlex Micro)
Prozessor	4 Kerne, aktuelle Generation	6 Kerne oder mehr
Arbeitsspeicher	16 GB	32 GB
System-SSD	256 GB NVMe	512 GB NVMe
Daten-SSDs	2 gleiche NVMe-SSDs je 1 TB, getrennt vom System	2 × 2 TB mit hoher Schreibfestigkeit (z. B. Samsung 990 Pro, ≥ 1.200 TBW)
Sicherheitschip	TPM 2.0, Secure Boot (UEFI)	–
Netzwerk	1 GbE kabelgebunden	–; WLAN wird nicht genutzt
USV	USV mit USB-Anschluss, von NUT unterstützt	APC Back-UPS 700–750 VA
Betriebssystem	kein Windows nötig – die Platten werden vollständig neu eingerichtet	Gerät möglichst ohne Windows-Lizenz bestellen

B2 · Firmware-Einstellungen (BIOS/UEFI)

- Secure Boot **an**, TPM 2.0 **an**.
- Nach Stromausfall: **einschalten** („After Power Loss: Power On“).
- Start von der System-SSD; Fast Boot **aus**; herstellerspezifische Sonderfunktionen, die Secure Boot verändern, aus.
- Ein Firmware-Passwort ist willkommen; es wird bei der IT des Kunden verwahrt.

B3 · Netzwerk und Standort

- Fester LAN-Anschluss, feste IP-Adresse oder DHCP-Reservierung.
- Ausgehend ins Internet: HTTPS (TCP 443) und UDP für Tailscale (41641 sowie 3478/STUN). **Keine** eingehende Portfreigabe am Router.
- Aus dem Büro-LAN zur Box: TCP 443 (docMan im Browser).
- Abschließbarer, belüfteter Platz; Box und USV an einem eigenen Stromkreis, wenn möglich.

B4 · Ablauf bis zur Inbetriebnahme

1. **Bereitstellung durch den Kunden:** Hardware nach B1, Einstellungen nach B2, Anschluss nach B3. Die IT installiert Ubuntu Server (von uns vorgegebene LTS-Version) mit OpenSSH und meldet das Gerät mit einem einmaligen Schlüssel, den wir schicken, in unserem Tailscale-Netz an. Alternativ liefern wir einen USB-Stick, der das ohne Rückfragen erledigt.
2. **Fernprüfung durch uns:** Wir prüfen aus der Ferne Prozessor, Speicher, SSDs (Modell, Größe, Zustand), TPM und Secure Boot, Netzwerk und USV-Anbindung und schicken einen Prüfbericht. Passt etwas nicht, steht darin, was zu ändern ist.

3. **Freigabe:** Erst wenn der Prüfbericht ohne offene Punkte ist, geht es weiter. Vorher wird nichts auf den Datenplatten eingerichtet.
4. **Erstinstallation durch uns:** Spiegel, Verschlüsselung mit TPM, Firewall, Abschottung, USV, docMan und Sicherung – wie in Teil A. Den Notfallschlüssel erzeugt der Kunde (oder seine IT) selbst und verwahrt ihn.
5. **Abnahme:** Wir führen die Prüfliste aus A7 durch (Neustart, Stromausfall, SSD-Ausfall, Sicherung und Wiederherstellung) und übergeben das Protokoll. Danach beginnt der Betrieb.

B5 · Wer ist wofür zuständig

Aufgabe	Kunde / IT des Kunden	docMan
Hardware, Garantie, Austausch defekter Teile	✓	meldet Defekte (z. B. SSD-Warnung)
Strom, USV, Netzwerk, Standort	✓	–
Notfallschlüssel verwahren	✓	–
Betriebssystem, Updates, Sicherheitseinstellungen	–	✓
docMan, Datenbank, Sicherung, Überwachung	–	✓
Benutzer und Rechte in docMan	✓ (Admin des Kunden)	hilft bei der Einrichtung

Änderungen an der Box außerhalb dieser Aufteilung bitte vorher absprechen – etwa zusätzliche Software, Virenscanner oder Monitoring-Agenten, damit Abschottung und Verschlüsselung nicht unbemerkt geschwächt werden.