Historie und Gültigkeit

- Gültiger Stand und Verlauf

Gültiger Stand und Verlauf

> Zielgruppe: Anwender und Betreuer · Stand: 06.11.2026

OpenBao ist der Secret-Store und die zentrale Zertifizierungsstelle (CA) der DEXPRO-Plattform. Diese Seite zeigt, was heute gilt, was noch offen ist und wie es dazu kam. Details findest du auf den Seiten der einzelnen Kapitel.

> OpenBao läuft bisher nur im **Lab** (Lab-PoC). Eine DEV- und eine Produktionsumgebung sind geplant, aber noch nicht aufgebaut.

Gültiger Stand

- **Entscheidung** (29.10.2026): OpenBao wird zentrale CA und Secret-Store der Plattform. Das Lab läuft als Cluster aus drei Knoten mit Raft-Storage und Static-Key-Seal.
- **Entscheidung** (29.10.2026): Die Root-CA ist offline. Sie liegt nie auf einer VM, nie im Terraform-State und nie in OpenBao. In OpenBao liegen nur Intermediate-CAs, je Zweck ein eigener PKI-Mount (z. B. für Consul).
- **Entscheidung** (30.10.2026): Secrets liegen in einem KV-v2-Mount je Abteilung (`cci/`, `cpi/`, `cpcs/`, `cpds/`) nach dem Schema `<abt>/<team>/<stage>/…` für Team-Secrets und `<abt>/shared/<stage>/…` für Secrets der ganzen Abteilung. Secrets von Nomad-Jobs liegen unter `<abt>/<team>/<stage>/nomad/<job>/…`. Die Stage-Segmente heißen wie die Branches (`pre-development`, `development`, `staging`, `production`).
- **Entscheidung** (02.11.2026): Ausnahme für die Abteilung CCI (Cloud Core Infrastructure): CCI ist **ein** Team und gliedert sich nach Standort und Projekt: `cci/shared/<stage>/…` (abteilungsweit), `cci/<standort>/<stage>/shared/…` (je Standort, z. B. `bremen1`) und `cci/<standort>/<stage>/<projekt>/…` (nur dieses Projekt schreibt). Die anderen Abteilungen bleiben teambasiert.
- **Konzept** (30.10.2026): Stage und Team ergeben sich bei Pipelines aus dem GitLab-JWT (Branch bzw. GitLab-Gruppe), bei Menschen aus ihrer Entra-Gruppe. Production-Secrets gibt es nur für geschützte Branches.
- **Regel** (30.10.2026): Ein Team liest den eigenen Teampfad und `shared/` seiner Abteilung. In `shared/` schreiben nur Menschen der Abteilung. Ausnahme CCI (02.11.2026): CCI-Pipelines dürfen auch in beide `shared`-Ebenen schreiben. Endgültig löschen (`destroy`) dürfen nur Menschen. Je Secret bleiben drei Versionen erhalten.
- **Entscheidung** (30.10.2026): Pipelines melden sich per GitLab-JWT an, VMs per AppRole mit an die Host-IP gebundener Secret-ID. Menschen nutzen im Lab ein Admin-Token, in DEV später OIDC mit Entra ID.

- **Entscheidung** (30.10.2026): Pipeline-Tokens leben kurz (15 Minuten, höchstens 1 Stunde). Rechte entstehen nur über JWT-Rolle und Policy.
- **Regel** (06.11.2026): Secrets entstehen nur auf zwei Wegen: Menschen legen sie nach dem OIDC-Login in der Oberfläche an, Pipelines schreiben sie mit ihrem GitLab-JWT. Bis OIDC mit DEV kommt, entstehen Secrets im Lab nur über Pipelines.
- **Regel** (30.10.2026): OpenBao ist nur intern erreichbar und **nie über den Edge**. Ohne Token sind nur die öffentlichen CA-Daten abrufbar (CA-Zertifikat, Kette, Sperrliste).
- **Regel** (30.10.2026): Der Stack, der OpenBao selbst baut, bezieht seine Zugänge aus Bitwarden und nie aus OpenBao. Sonst ließe sich OpenBao nach einem Ausfall nicht wieder aufbauen. Das gilt auch für jeden späteren Produktions-, Restore- oder Bootstrap-Stack.
- **Entscheidung** (30.10.2026): Es wird kein externes Nomad-Secrets-Plugin eingesetzt. Pipelines sprechen Nomad über dessen eigene JWT-Anmeldung an, ohne Umweg über OpenBao.
- **Entscheidung** (30.10.2026): Bitwarden-Inhalte ziehen schrittweise nach OpenBao um, in dieser Reihenfolge: Provider-Zugänge, von Modulen erzeugte Secrets, Ablösung von ssl-service, SSH-CA.
- **Fakt** (02.11.2026): Die Provider-Zugänge der Lab-Stacks (Proxmox, PowerDNS, NetBox, CheckMK, hosttech) liegen in OpenBao. Eine Lab-Pipeline hat sie per GitLab-JWT gelesen, fremde Stages bleiben gesperrt. Die Originale bleiben vorerst in Bitwarden.
- **Entscheidung** (02.11.2026): Von Modulen erzeugte Secrets (z. B. Datenbank-Accounts) ziehen in zwei Stufen um. Zuerst bekommt jedes Modul einen Schalter mit Bitwarden als Default. Danach folgt je Modul eine neue Version, die nur noch OpenBao kennt.
- **Fakt** (02.11.2026): Die Lab-Consul-Server wurden mit Zertifikaten aus OpenBao neu aufgebaut (siehe Kapitel PKI).

Offen

- **Offen**: Aufbau von OpenBao in DEV und Produktion, inklusive Seal-Verfahren und automatischer Snapshots außerhalb der Knoten
- **Offen**: Anmeldung für Menschen per OIDC mit Entra ID (DEV)
- **Offen**: Von Modulen erzeugte Secrets in OpenBao ablegen (Plan steht, Start nach dem Pilot mit dem Lab-Edge-Stack)
- **Offen**: Lab-Zugänge in die Standort-Ebene umziehen (`cci/bremen1/<stage>/shared/…`), anschließend die bisherige Sammelrolle ablösen
- **Offen**: ssl-service durch die OpenBao-PKI ersetzen
- **Offen**: SSH-User- und Host-CA über OpenBao (später)
- **Offen**: Abschluss des Consul-Neubaus: Die ACL-Einrichtung hängt noch an der abgebauten Lab-Nomad-Anmeldung
- **Offen**: Erneuerung des Listener-Zertifikats absichern (Reload-Test und Überwachung, aktuelles Zertifikat gilt bis 04.12.2026)
- **Offen**: Consul-Connect-CA und Nomad-TLS über OpenBao

- **Offen**: Konfiguration als Code: Mounts, Policies und Rollen aus einer Team-Liste per Terraform erzeugen

Verlauf

- **Regel** (06.11.2026): Secrets nur per OIDC-Login in der Oberfläche oder per GitLab-JWT in der Pipeline anlegen.
- **Fakt** (02.11.2026): Lab-Consul-Server über die OpenBao-PKI neu aufgebaut.
- **Entscheidung** (02.11.2026): CCI-Gliederung nach Standort und Projekt (siehe Gültiger Stand). *Überholt:* Team-Segment für CCI, z. B. `bremen1` als Team.
- **Entscheidung** (02.11.2026): Umzug der Modul-Secrets zweistufig per Schalter.
- **Fakt** (02.11.2026): Provider-Zugänge der Lab-Stacks aus OpenBao abgeschlossen und im Testlauf nachgewiesen.
- **Fakt** (30.10.2026): Die Firewall von den GitLab-Runnern zu OpenBao (Port 8200) ist offen. Der Pipeline-Login per GitLab-JWT ist nachgewiesen. Davor erreichten die Runner OpenBao nicht.
- **Entscheidung** (30.10.2026): Kurswechsel bei der Consul-Pipeline: Sie meldet sich per GitLab-JWT an statt mit einem langlebigen Bootstrap-Token. *Überholt:* Bootstrap-Token als CI-Variable.
- **Entscheidung** (30.10.2026): Endfassung des Pfadschemas (siehe Gültiger Stand). *Überholt:* ein gemeinsamer Mount `kv/` mit Stages `lab/dev/stg/prd`, Stage vor dem Team im Pfad sowie Stage aus Projektpfad oder Metadaten.
- **Fakt** (30.10.2026): Root-Token im Lab widerrufen. Seitdem gibt es ein Admin-Token und ein Reserve-Token (Break-glass).
- **Entscheidung** (30.10.2026): OpenBao-Knoten bekommen im VM-Modul eine eigene Rolle und werden nicht in Consul registriert. *Überholt:* Umweg über Ansible-Tags.
- **Fakt** (29./30.10.2026): Lab-Cluster aufgebaut und initialisiert. HA-Test, Snapshot/Restore und Negativtest gegen den Edge sind bestanden.
- **Entscheidung** (29.10.2026): Lab-MVP von OpenBao als zentrale CA für den Lab-Nomad gestartet. Löst eine ältere OpenBao-Planung ab.

Weiterführend

- OpenBao-Dokumentation