Offline-Root-CA und Intermediates

> Zielgruppe: Betreuer · Stand: 06.11.2026

OpenBao ist die zentrale Zertifizierungsstelle (CA) der Plattform. Die Root-CA bleibt offline. In OpenBao arbeiten nur Intermediate-CAs, und zwar eine je Zweck. Diese Seite erklärt den Aufbau und warum er so gewählt ist.

> **Lab-PoC:** Bisher gibt es die Root-CA des Labs und ein Intermediate für Consul.

Aufbau

Ebene	Wo	Laufzeit	Eigenschaften
Root-CA	offline, nie auf einer VM, nie im Terraform-State, nie in OpenBao	10 Jahre	ECDSA P-384, darf nur eine Ebene Intermediates signieren
Intermediate je Zweck	eigener PKI-Mount in OpenBao, z. B. `pki-consul`	3–5 Jahre	Schlüssel verlässt OpenBao nie, Namen per Name Constraints begrenzt
Zertifikate (Leaf)	auf den Hosts	kurz, z. B. Consul 30 Tage	werden automatisch erneuert

Geplante weitere Intermediates: Nomad-TLS und Consul-Connect.

Wie ein Intermediate entsteht

1. OpenBao erzeugt im neuen PKI-Mount Schlüssel und CSR. Der Schlüssel bleibt in OpenBao.
2. Die Root-CA signiert die CSR offline auf einem abgeschotteten Rechner, in einem Speicher, der beim Ausschalten verschwindet.
3. Das signierte Zertifikat wird in OpenBao importiert.
4. Rollen im Mount legen fest, welche Namen und IPs Zertifikate bekommen dürfen.

Der Root-Schlüssel ist verschlüsselt in Bitwarden gesichert und wird nur zum Signieren kurz geladen.

Öffentliche CA-Daten

CA-Zertifikat, Kette und Sperrliste eines Mounts sind ohne Token abrufbar, z. B. für Clients, die der CA vertrauen sollen:

```
curl -s https://openbao-lab-bre1.dexpro.parts:8200/v1/pki-consul/ca_chain
```

Stolperfallen

> IP-Adressen in Rollen begrenzt nur das Feld `allowed_ip_sans_cidr`. Ein Feld `allowed_ip_sans` wird still ignoriert, und `allow_ip_sans=true` allein erlaubt beliebige IPs. Nach jeder Rollenänderung mit einer unerlaubten IP gegenprüfen (Erwartung: HTTP 400).

- Läuft ein Intermediate ab, sind alle Zertifikate darunter wertlos. Die Restlaufzeit braucht deshalb eine Überwachung.
- Leaf-Zertifikate sollen alarmieren, wenn sie weniger als 14 Tage gelten.

Weiterführend

- Consul-Zertifikate aus OpenBao
- OpenBao: PKI Secrets Engine

Revision #1
Created 2026-11-06 17:42:18 UTC by Alexander Golembek
Updated 2026-11-06 17:42:18 UTC by Alexander Golembek