LUKS2 und dm-crypt

Installation (Debian)

```
sudo apt update
```

```
sudo apt install cryptsetup
```

Installation prüfen:

```
cryptsetup --version
```

Einordnung

`dm-crypt` ist die Verschlüsselungsschicht des Linux-Kernels. LUKS ist ein standardisiertes Format zur Verwaltung verschlüsselter Datenträger und ihrer Schlüssel-Slots. LUKS2 ist die moderne Formatgeneration.

Siehe auch unter Tuxedo-Computers

Informationen prüfen

Vor jedem Befehl das korrekte Blockgerät identifizieren:

```
lsblk -f
```

Headerinformationen anzeigen:

```
sudo cryptsetup luksDump /dev/sdX1
```

`/dev/sdX1` ist nur ein Platzhalter. Die Abfrage `luksDump` zeigt Metadaten, keine entschlüsselten Nutzdaten.

Bestehenden LUKS-Datenträger öffnen

```
sudo cryptsetup open /dev/sdX1 sicher
```

Mountverzeichnis anlegen (sofern nicht vorhanden):

```
sudo mkdir -p /mnt/sicher
```

Dateisystem einhängen:

```
sudo mount /dev/mapper/sicher /mnt/sicher
```

Nach der Verwendung:

```
sudo umount /mnt/sicher
```

Erst nach dem Aushängen das LUKS-Volume schließen:

```
sudo cryptsetup close sicher
```

Vorsicht: Gerätebezeichnungen und Mountpunkte müssen zur tatsächlichen Umgebung passen.

Schlüssel-Slots

LUKS kann mehrere Zugangsmöglichkeiten zum selben Volume-Schlüssel verwalten. Passphrasen lassen sich ergänzen oder entfernen. Vor Änderungen muss eine funktionierende alternative Entsperrmethode geprüft sein.

Header-Sicherung

Der LUKS-Header enthält für die Entschlüsselung unverzichtbare Metadaten. Ein Header-Backup ist äußerst sensibel und muss geschützt werden:

```
sudo cryptsetup luksHeaderBackup /dev/sdX1 --header-backup-file luks-header.img
```

Wichtig: Der Header kann Zugang zu den verschlüsselten Daten erleichtern und ist bei späteren Änderungen möglicherweise veraltet. Die Datei sicher und getrennt vom Datenträger aufbewahren.

Sicherheitsaspekte

LUKS schützt Daten vor allem im ausgeschalteten Zustand. Ein entsperrtes System bietet diesen Schutz gegenüber laufenden Prozessen nicht. Auch unverschlüsselte Boot-Komponenten und die Integrität des Systems sind zu berücksichtigen.

Zurück zur Übersicht

From:
https://wiki.bluegnu.de/ - **wiki**

Permanent link:
https://wiki.bluegnu.de/doku.php/open:it:secure:luks

Last update: **2026/11/15 17:53**