

# Crypsetup

Tiré de <https://www.thegeekstuff.com/2016/03/cryptsetup-lukskey/>.

## Identifier la partition chiffrée

```
sudo lsblk -o name,size,fstype,label,mountpoint
```

Chez moi, ça donne ça :

| NAME             | SIZE   | FSTYPE      | LABEL | MOUNTPOINT |
|------------------|--------|-------------|-------|------------|
| sda              | 238.5G |             |       |            |
| └─sda1           | 512M   | vfat        |       | /boot/efi  |
| └─sda2           | 244M   | ext2        |       | /boot      |
| └─sda3           | 237.7G | crypto_LUKS |       |            |
| └─sda3_crypt     | 237.7G | LVM2_member |       |            |
| └─foo--vg-swap_1 | 6.8G   | swap        |       | [SWAP]     |
| └─foo--vg-root   | 27.9G  | ext4        |       | /          |
| └─foo--vg-home   | 203G   | ext4        |       | /home      |

La partition chiffrée est donc `/dev/sda3`.

## Identifier les slots de clés déjà utilisés

On peut avoir 8 clés de chiffrement, chacune occupant un *slot*.

```
sudo cryptsetup luksDump /dev/sda3 | grep Slot
```

Chez moi, ça donne :

```
Key Slot 0: ENABLED
Key Slot 1: DISABLED
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED
```

## Ajouter une nouvelle clé

```
sudo cryptsetup luksAddKey /dev/sda3
```

Cryptsetup vous demandera alors de taper la *passphrase* d'une des clés existantes puis de taper (deux fois) une nouvelle *passphrase* pour la nouvelle clé.

On peut forcer le slot pour la nouvelle clé :

```
sudo cryptsetup luksAddKey /dev/sda3 -S 4
```

## Supprimer une clé

```
sudo cryptsetup luksRemoveKey /dev/sda3
```

Cryptsetup vous demandera alors de taper la *passphrase* de la clé à supprimer. Je ne sais pas ce qui se passerait si la *passphrase* était utilisée pour plusieurs clés (je ne sais même pas si c'est possible).

Si on a oublié la *passphrase* de la clé à supprimer, on peut supprimer son slot :

```
cryptsetup luksKillSlot /dev/sda3 2
```

Cryptsteup vous demandera alors de taper la *passphrase* d'une des clés existantes.

---

Révision #1

Créé 2022-11-23 16:59:15 CET par Luc

Mis à jour 2023-08-21 09:10:56 CEST par Luc