How to change LUKS disk encryption passphrase in Linux

We use encryption to protect mobile devices. For instance, I always use LUKS disk encryption to protect all files stored on my SSD. Dm-crypt (Cryptsetup and LUKS) open-source disk encryption is transparent disk encryption and a great way to keep your data secure. However, changing passphrase is a bit of a challenge for new Linux users and developers. This step-by-step guide explains how to find LUKS slots assigned to you and change your passphrase on a Debian/Ubuntu, CentOS/RHEL, OpenSUSE/SUSE other Linux distros.

How to change LUKS disk encryption passphrase in Linux

First, we need to locate information about encrypted filesystems.

Step 1 – Query /etc/crypttab file on Linux

The file /etc/crypttab contains descriptive information about LUKS encrypted filesystems and view with the cat command:

```
# sudo cat /etc/crypttab
```

Here is what I saw:

```
sda3_crypt UUID=42e50ed0-5055-45f5-b1fc-0f54669e6d1f none luks,discard>
```

So I have sda3_crypt. On your system, you may see a different name such as `md1_crypt` for RAID-1 protected LUKS disk encryption. Now we obtained device information, and it is time to find the partition schema for sda3:

```
# sudo fdisk -l /dev/sda
```

Outputs:

```
Disk /dev/sda: 931.5 GiB, 1000204886016 bytes, 1953525168 sectors
Disk model: CT1000MX500SSD1
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disklabel type: gpt
Disk identifier: 1BB1DDD0-47F9-48FB-AA29-69D6A74F4D91

Device       Start        End    Sectors   Size Type
/dev/sda1     2048    1050623    1048576   512M EFI System
/dev/sda2  1050624    1550335     499712   244M Linux filesystem
```

```
/dev/sda3  1550336 1953523711 1951973376 930.8G Linux filesystem
```

Make sure you substitute /dev/sda3 with your actual device name on Linux.

Step 2 – Dump the header information of a LUKS device

Execute the following command to get information about our encrypted /dev/sda3:

```
# sudo cryptsetup luksDump /dev/sda3
```

My LUKS disk/parition header info:

```
LUKS header information
Version:        2
Epoch:          4
Metadata area:  16384 [bytes]
Keyslots area:  16744448 [bytes]
UUID:           42e50ed0-5055-45f5-b1fc-0f54669e6d1f
Label:          (no label)
Subsystem:      (no subsystem)
Flags:          (no flags)

Data segments:
  0: crypt
    offset: 16777216 [bytes]
    length: (whole device)
    cipher: aes-xts-plain64
    sector: 512 [bytes]

Keyslots:
  0: luks2
    Key:        512 bits
    Priority:   normal
    Cipher:     aes-xts-plain64
    Cipher key: 512 bits
    PBKDF:      argon2i
    Time cost:  7
    Memory:     1048576
    Threads:    4
    Salt:       fc 9d b7 e0 ec 06 d0 b1 47 09 61 6f c1 73 f9 51
                b7 ff 9b 6b 44 a0 2b c5 dd 5a c4 7e 46 28 c3 62
    AF stripes: 4000
    AF hash:    sha256
    Area offset:32768 [bytes]
    Area length:258048 [bytes]
    Digest ID:  0
```

```
Tokens:
Digests:
  0: pbkdf2
    Hash:       sha256
    Iterations: 136107
    Salt:       40 82 65 fc cf e1 24 d3 0d b8 85 07 13 c7 dd a1
                03 52 6a b9 04 b8 6d 23 4a d1 90 89 cb 96 a7 ca
    Digest:     5b d0 10 56 e4 9a ff e1 eb 14 2a fb 4d 85 ba c3
                a7 75 fa fa 6c 24 cc 01 b0 9c 34 dd 48 98 1a d9
```

It seems I only have slot 0, but on many systems, you may see up to 8 slots numbered from 0 to 7. Therefore in step # 3, we will see how to determine your LUKS slot.

Step 3 – Finding out LUKS slot assigned to you by Linux sysadmin or installer

To determine which luks slot a passphrase is in on Linux, run:

```
# sudo cryptsetup --verbose open --test-passphrase /path/to/dev/
# sudo cryptsetup --verbose open --test-passphrase /dev/sda3
```

The command will tell you the correct LUKS slot without any guesswork on your part:

```
Enter passphrase for /dev/sda3:
Key slot 0 unlocked.
Command successful.
```

Please note down slot number. In other words, we need to use slot number 0 for /dev/sda3.

Step 4 – Changing LUKS disk encryption passphrase in Linux using the command-line

So far, so good we obtained all information required for updating or changing or existing passphrase. Please note that a passphrase is similar to a password in usage but is commonly longer for security reasons. The syntax is:

```
# sudo cryptsetup luksChangeKey /dev/sda3 -S 0
```

First, enter the existing passphrase and press the `[Enter]` key. If the passphrase is correct, you are allowed to change it by entering it twice as follows:

```
Enter passphrase to be changed:
Enter new passphrase:
Verify passphrase:
```

Step 5 – Verify new passphrase

Either reboot the Linux system or simulate a new passphrase on the CLI as follows:

```
# sudo cryptsetup --verbose open --test-passphrase /dev/sda3
```