Notizen zur Verschlüsselung von USB-Sticks

Zielsetzung:
Ein USB-Laufwerk soll mit LUKS so verschlüsselt werden, dass es bei Bedarf wieder möglichst einfach im Debian-System verfügbar gemacht werden kann.

Ergebnisse:
Zuerst wird die Partitionierung des Laufwerks mit GParted so konfiguriert, dass außer den anderen (später nicht verschlüsselten) Partitionen eine weitere Partition registriert ist. Wichtig ist, dass der Bereich nicht einfach nur „freier Speicher“ sein darf, denn dieser lässt sich nicht über */dev/sd**X*** ansprechen. Um Angriffe auf die Verschlüsselung zu erschweren, wird nun die Partition mit Zufallsdaten beschrieben:

```
dd if=/dev/urandom of=/dev/sdX bs=4K
```

Für die Verschlüsselung muss das Kernelmodul „dm_crypt“ geladen sein. Wird es nicht immer automatisch beim Start geladen, registriert und lädt man es einmalig:

```
echo dm_crypt >> /etc/modules
modprobe dm_crypt
```

Damit ist nun alles bereit, um die ausgewählte Partition nun nach der Vergabe eines Passworts durch eine zusätzliche Schicht zu verschlüsseln:

```
cryptsetup -yvh sha256 -c aes-xts-plain -s 256 luksFormat /dev/sdX
```

Nun kann das Dateisystem nach der Bereitstellung der LUKS-Partition als virtuelles Gerät unter */dev/maper/**X*** wie gewohnt formatiert werden! Später wird das Mapping beim Anschluss des Laufwerks (zumindest im Fall von KDE) automatisch gemacht. Für die erste Einrichtung kann man jedoch einmal manuell die Partition bereitstellen:

```
cryptsetup luksOpen /dev/sdX geheim
```

Durch den obigen Befehl wurde nun Zugriff auf die Partition durch die zusätzliche Schicht mittels */dev/mapper/geheim* erlaubt. Hier muss man nun aufpassen, dass man nicht mehr */dev/sd**X*** direkt anspricht, denn über diesen Weg bekommt man lediglich Zugriff auf den „Schlüsseltext“, also die rohen Daten der Partition. Nächster Schritt ist dann das Anlegen eines Dateisystems auf */dev/mapper/geheim*, bestenfalls ext4.

```
mkfs.ext4 /dev/mapper/geheim
```

Bevor man das neu erstellte Dateisystem nun einhängt, sollte man jedoch je nach Situation einige weiterführende Optimierungen beachten! Im Fall von ext4 wird ein fixer Prozentsatz des verfügbaren Speichers gegen Fragmentierung und für den Notfall reserviert, jedoch ist das bei Laufwerken, die nur als Datenspeicher für Dateien normaler Größe genutzt werden, eigentlich nicht nötig.

Um also etwas mehr Speicher nutzen zu können, kann man mit folgendem Befehl dem Dateisystem zum Beispiel mitteilen, dass kein Speicher reserviert werden soll:

```
tune2fs -m 0 /dev/mapper/geheim
```

Außerdem hat das Dateisystem möglicherweise noch keinen Namen. Wenn man jedoch nicht später unter */dev/mapper/* die Partition nach ihrer UUID benannt haben möchte, empfiehlt sich die Umbenennung des Dateisystems:

```
e2label /dev/mapper/geheim IntuitiverName
```

Achtung: Der Name darf maximal 16 Zeichen lang sein. Doch nun kann man endlich das Dateisystem das erste Mal einhängen und gleich den Besitzer ändern:

```
mount /dev/mapper/geheim /mnt
chown -R user:user /mnt
```

Nachdem nun alles bereit ist, kann das manuelle Mapping aufgehoben werden:

```
umount /mnt
cryptsetup luksClose /dev/mapper/geheim
```

Damit ist die Partition nun auf höchstem Niveau verschlüsselt! Ab jetzt sollte KDE beim Anschluss des Laufwerks die Möglichkeit zur Eingabe des Passworts geben. Wer sich nun noch darüber ärgert, dass die Partition als „**X** GiB Wechseldatenträger“ in KDE angezeigt wird, dem kann eine udev-Regel zur richtigen Benennung helfen:

```
KERNEL=="sd*", ENV{ID_FS_UUID}=="UUID_DER_VERSCHLÜSSELTEN_PARTITION",
ENV{ID_FS_LABEL}="TOLLER_NAME", ENV{ID_FS_LABEL_ENC}="TOLLER_NAME"
```

Die UUID der Partition lässt sich einfach mit „blkid“ herausfinden. Die udev-Regel muss dann in einer Datei mit der Endnung *.rules* und einem möglichst vielsagenden Namen im Ordner */lib/udev/rules.d/* abgelegt werden. Es empfiehlt sich zum Beispiel eine gemeinsame Datei mit allen Regeln für verschlüsselte Partitionen. Nach einem Neustart des udev-Dienstes wird nun auch der Name in KDE schön angezeigt!

```
/etc/init.d/udev restart
```

Referenzen:

[Linux-community.de] Anwendung von LUKS unkompliziert erklärt
[Linuxundich.de] Warum ist die ext4-Partition kleiner als angegeben?
[Ubuntuusers.de] Einige sehr nützliche Tipps zum Umgang mit udev