2025/12/06 12:54 1/4 Le chiffrement sous linux

## Le chiffrement sous linux

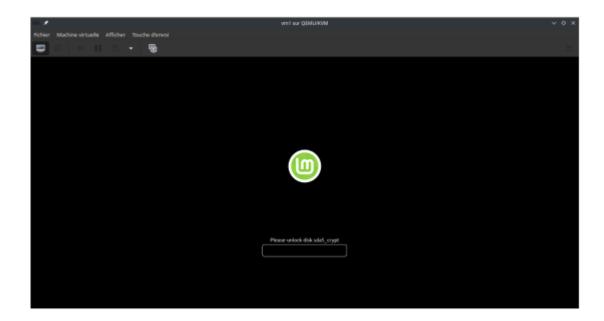
## **Quelques définitions**

Chiffrer des données est l'action de rendre des données illisibles si on ne dispose pas d'un secret précis, la clé.

On va parler ici de chiffrement symétrique, c'est à dire que la clé servant à déchiffrer est la même que celle servant à chiffrer.

Pour plus d'informations.

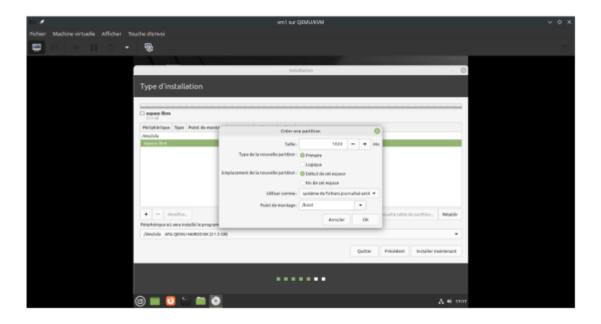
## Partie 1: le chiffrement disque entier



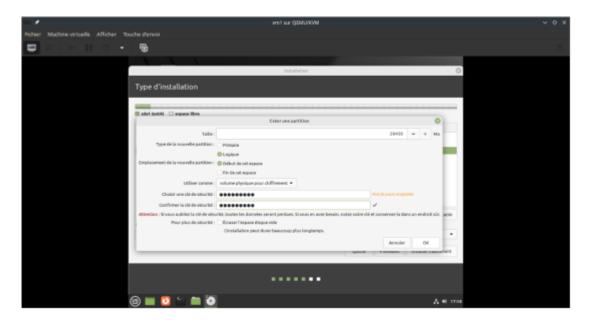
Il va s'agir ici de chiffrer l'intégralité du disque dur de l'ordinateur. On parle alors de full disk encryption.

Ce chiffrement se fait à l'installation. On va créer 2 partitions, une pour le /boot et une autre pour le volume chiffré. Actuellement, l'installateur de Linux Mint ne propose que d'installer en une partiton "/", une configuration avec LVM doit être faite à la main.

On créé la partiton de boot



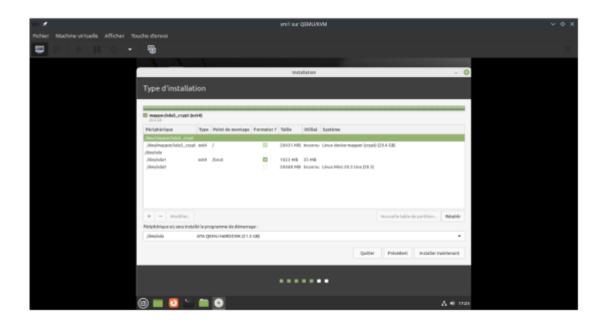
On créé la partition contenant le volume chiffré



On sélectionne le volume pour y placer la racine

https://wiki.alpinux.org/ Printed on 2025/12/06 12:54

2025/12/06 12:54 3/4 Le chiffrement sous linux



L'ordinateur va demander le mot de passe à chaque démarrage.



#### **Avantages**

On évite d'exposer la structure du FS comme avec un chiffrement par fichier.

#### **Inconvénients**

Ralentit l'ordinateur.

#### Comment gérer le multi-utilisateur

On peut rajouter des clés dans le trousseau de LUKS avec

cryptsetup luksAddKey /dev/sdX

https://access.redhat.com/solutions/230993

### Partie 2: Chiffrement des volumes "mobiles"

## **LUKS**

https://geekyshacklebolt.wordpress.com/2019/03/06/how-to-encrypt-usb-drives-with-luks/

# **Veracrypt**

https://www.veracrypt.fr/code/VeraCrypt/

From:

https://wiki.alpinux.org/ - Alpinux Wiki

Permanent link:

https://wiki.alpinux.org/technique/pratique/chiffrement?rev=1683828370

Last update: 2023/05/11 20:06



https://wiki.alpinux.org/ Printed on 2025/12/06 12:54