

GNU / LINUX

Encryption du FS

LUKS — cryptsetup — partitions cryptées

LUKS

dm-crypt

cryptsetup

Sommaire

1. Objectifs
2. LUKS
3. Architecture
4. Support physique et mapper
5. Installation et vérification
6. Préparation du disque

1. GNU / Linux – Encryption du FS

Objectifs

- Comprendre l'architecture de LUKS
 - Mapper
- Mettre en place des partitions cryptées
 - Partitionnement
 - Préparation des partitions
 - Ouverture / Fermeture des volumes
- Réaliser une installation d'une Debian cryptée
- Utilisation de LVM et de LUKS
 - Un mapper crypté au dessus d'un mapper de volumes

Cédric Chappert – C2LR – Tous droits réservés Formation Linux 3

2. GNU / Linux – Encryption du FS

LUKS

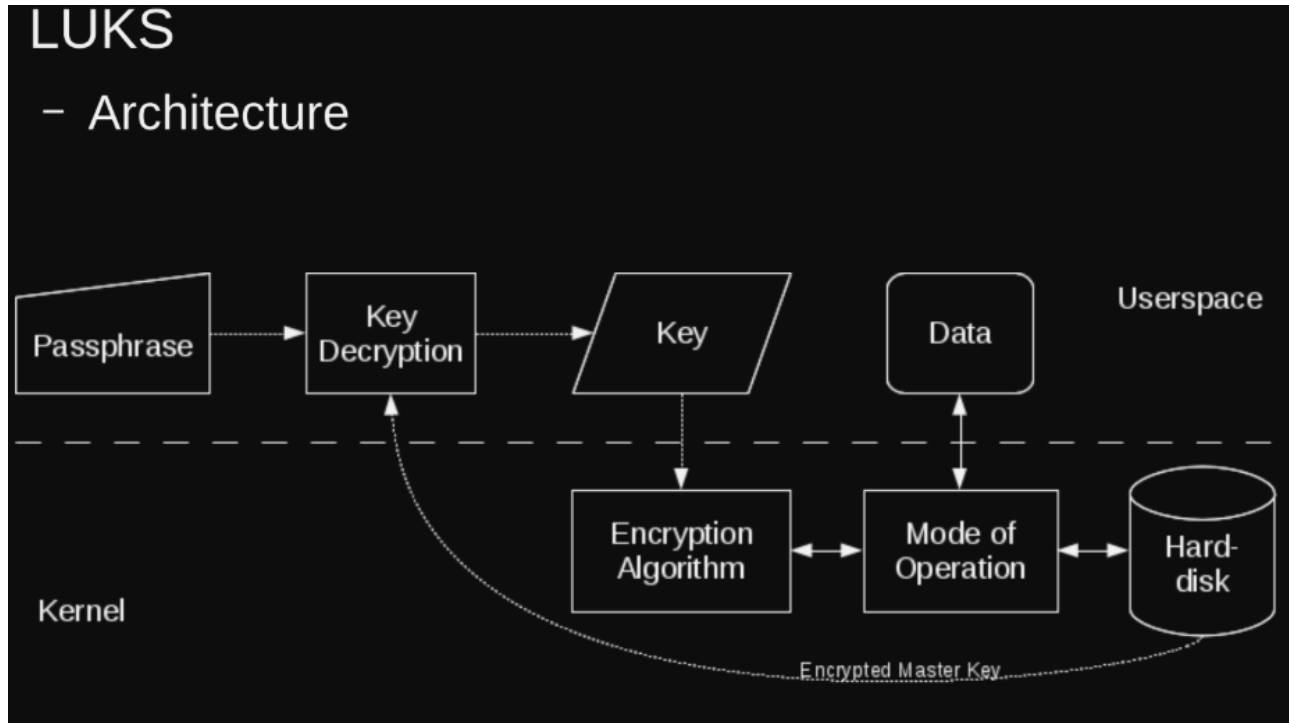
- Linux Unified Key Setup
- Standard de Linux
 - Dans le noyau
 - Chiffrement des disques et des partitions
- Encryption symétrique
 - Sur mot de passe
- Implémentation de référence : cryptsetup
 - <https://gitlab.com/cryptsetup/cryptsetup>
 - <https://gitlab.com/cryptsetup/LUKS2-docs/-/blob/main/>
 - luks2_doc_wip.pdf

Cédric Chappert – C2LR – Tous droits réservés Formation Linux 4

3. GNU / Linux – Encryption du FS

LUKS

– Architecture

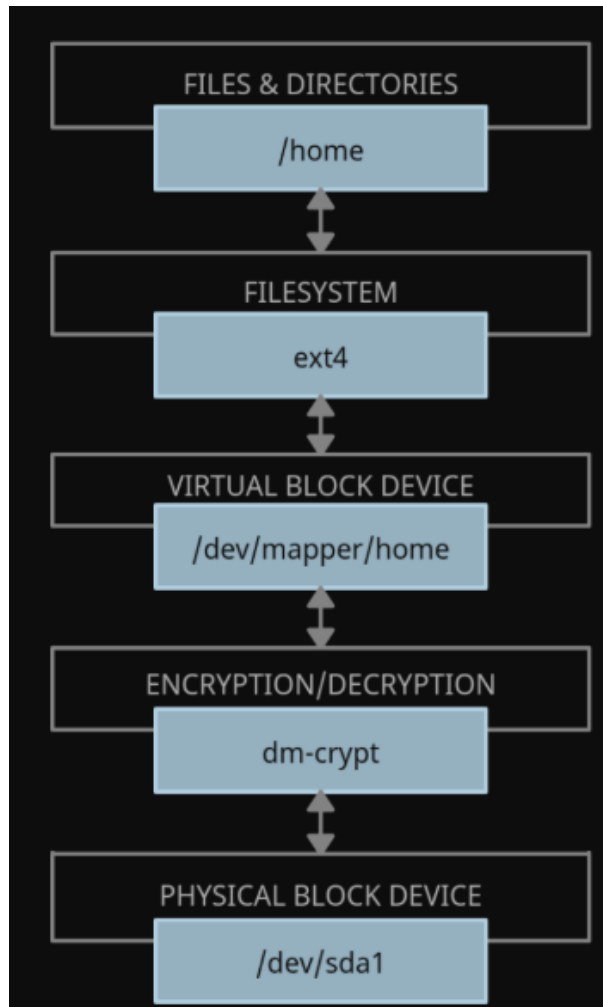


Cédric Chappert – C2LR – Tous droits réservés Formation Linux 5

4. GNU / Linux – Encryption du FS

LUKS

- Support physique et mapper
 - Le support est crypté
- dm-crypt s'occupe de la crypto
 - le mapper
 - expose le périphérique
 - décrypté
- Le Userland utilise le FS
 - De manière transparente



Cédric Chappert – C2LR – Tous droits réservés Formation Linux 6

5. GNU / Linux – Encryption du FS

LUKS

```
# Installation
apt-get install cryptsetup
# Vérification des algorithmes
# Affichage de tous les algo avec les performances
cryptsetup benchmark
# aes-cbc est très rapide en déchiffrement
# aes-xts avec une clé 256b est un bon compromis
# On peut utiliser une clé usb ou un disque virtuel
cryptsetup luksDump /dev/sde1
/dev/sde1 n'est pas un périphérique LUKS valide.
# J'utilise /dev/sde pour la suite
```

Cédric Chappert – C2LR – Tous droits réservés Formation Linux 7

6. GNU / Linux – Encryption du FS

LUKS

```
# Préparation du disque
fdisk /dev/sde
# d > n > p > 1 > ENTER > ENTER > w
# A vous de jouer avec les TD
# 18_Linux_-_File_systems_Encryption-TD00.pdf
# 18_Linux_-_File_systems_Encryption-TD01.pdf
# Pour installer une debian chiffrée
# 18_Linux_-_File_systems_Encryption-TD02.pdf
# Pour chiffrer par dessus LVM
# 18_Linux_-_File_systems_Encryption-TD03.pdf
```