

# Chiffrement

Rochelug

Philippe Harrand

17 septembre 2009



# Chiffrement des partitions



# Généralités chiffrement Linux

- ▶ **chiffrement des partitions**
  - ▶ contenant des données sensibles
  - ▶ ainsi que la partition swap
  - ▶ création du système de fichiers sur la partition chiffrée
  - ▶ par défaut chiffrement AES avec clef 128 bits

# Généralités chiffrement Linux

- ▶ chiffrement des partitions
- ▶ **contenant des données sensibles**
- ▶ ainsi que la partition swap
- ▶ création du système de fichiers sur la partition chiffrée
- ▶ par défaut chiffrement AES avec clef 128 bits

# Généralités chiffrement Linux

- ▶ chiffrement des partitions
- ▶ contenant des données sensibles
- ▶ **ainsi que la partition swap**
- ▶ création du système de fichiers sur la partition chiffrée
- ▶ par défaut chiffrement AES avec clef 128 bits

# Généralités chiffrement Linux

- ▶ chiffrement des partitions
- ▶ contenant des données sensibles
- ▶ ainsi que la partition swap
- ▶ **création du système de fichiers sur la partition chiffrée**
- ▶ par défaut chiffrement AES avec clef 128 bits

# Généralités chiffrement Linux

- ▶ chiffrement des partitions
- ▶ contenant des données sensibles
- ▶ ainsi que la partition swap
- ▶ création du système de fichiers sur la partition chiffrée
- ▶ **par défaut chiffrement AES avec clef 128 bits**

# Criptsetup LUKS

## ▶ **Linux Unified Key Setup**

- ▶ utilisé sur un volume "physique" logique
- ▶ avant création du système de fichiers
- ▶ fournissez une *"phrase de passe"*
- ▶ à ne pas oublier !

# Criptsetup LUKS

- ▶ **Linux Unified Key Setup**
- ▶ **utilisé sur un volume "physique" logique**
- ▶ avant création du système de fichiers
- ▶ fournissez une *"phrase de passe"*
- ▶ à ne pas oublier !

# Criptsetup LUKS

- ▶ **Linux Unified Key Setup**
- ▶ utilisé sur un volume "physique" logique
- ▶ **avant création du système de fichiers**
  - ▶ fournissez une *"phrase de passe"*
  - ▶ à ne pas oublier !

# Criptsetup LUKS

- ▶ **Linux Unified Key Setup**
- ▶ utilisé sur un volume "physique" logique
- ▶ avant création du système de fichiers
- ▶ fournissez une *"phrase de passe"*
- ▶ à ne pas oublier !

# Criptsetup LUKS

- ▶ **Linux Unified Key Setup**
- ▶ utilisé sur un volume "physique" logique
- ▶ avant création du système de fichiers
- ▶ fournissez une *"phrase de passe"*
- ▶ **à ne pas oublier !**

# Préparation

- ▶ volume logique :

`/dev/sdb1`

- ▶ création volume chiffré :

```
cryptsetup luksFormat /dev/sdb1
```

- ▶ ouverture volume chiffré :

```
cryptsetup luksOpen /dev/sdb1 maClef
```

- ▶ création système de fichiers :

```
mkfs.ext2 /dev/mapper/maClef
```

- ▶ fermeture du volume :

```
cryptsetup luksClose maClef
```

# Préparation

- ▶ volume logique :

`/dev/sdb1`

- ▶ création volume chiffré :

```
cryptsetup luksFormat /dev/sdb1
```

- ▶ ouverture volume chiffré :

```
cryptsetup luksOpen /dev/sdb1 maClef
```

- ▶ création système de fichiers :

```
mkfs.ext2 /dev/mapper/maClef
```

- ▶ fermeture du volume :

```
cryptsetup luksClose maClef
```

# Préparation

- ▶ volume logique :

```
/dev/sdb1
```

- ▶ création volume chiffré :

```
cryptsetup luksFormat /dev/sdb1
```

- ▶ ouverture volume chiffré :

```
cryptsetup luksOpen /dev/sdb1 maClef
```

- ▶ création système de fichiers :

```
mkfs.ext2 /dev/mapper/maClef
```

- ▶ fermeture du volume :

```
cryptsetup luksClose maClef
```

# Préparation

- ▶ volume logique :

```
/dev/sdb1
```

- ▶ création volume chiffré :

```
cryptsetup luksFormat /dev/sdb1
```

- ▶ ouverture volume chiffré :

```
cryptsetup luksOpen /dev/sdb1 maClef
```

- ▶ création système de fichiers :

```
mkfs.ext2 /dev/mapper/maClef
```

- ▶ fermeture du volume :

```
cryptsetup luksClose maClef
```

# Préparation

- ▶ volume logique :

```
/dev/sdb1
```

- ▶ création volume chiffré :

```
cryptsetup luksFormat /dev/sdb1
```

- ▶ ouverture volume chiffré :

```
cryptsetup luksOpen /dev/sdb1 maClef
```

- ▶ création système de fichiers :

```
mkfs.ext2 /dev/mapper/maClef
```

- ▶ fermeture du volume :

```
cryptsetup luksClose maClef
```



# Utilisation

- ▶ **Insérer la clef et attendre un peu**
- ▶ GNOME (testé avec Lenny)
  - ▶ Dans la fenêtre qui s'ouvre taper la phrase de passe
- ▶ KDE (testé avec Mandriva 2008)
  - ▶ déterminer le volume :  
`ameg`
  - ▶ ouverture du volume chiffré :  
`cryptsetup luksOpen /dev/sdXX maClef`
- ▶ la fenêtre habituelle s'ouvre, utiliser la clef, démonter la clef

# Utilisation

- ▶ Insérer la clef et attendre un peu
- ▶ **GNOME (testé avec Lenny)**
  - ▶ Dans la fenêtre qui s'ouvre taper la phrase de passe
- ▶ KDE (testé avec Mandriva 2008)
  - ▶ déterminer le volume :  
`ameg`
  - ▶ ouverture du volume chiffré :  
`cryptsetup luksOpen /dev/sdXX maClef`
- ▶ la fenêtre habituelle s'ouvre, utiliser la clef, démonter la clef

# Utilisation

- ▶ Insérer la clef et attendre un peu
- ▶ GNOME (testé avec Lenny)
  - ▶ Dans la fenêtre qui s'ouvre taper la phrase de passe

- ▶ KDE (testé avec Mandriva 2008)

- ▶ déterminer le volume :

- ame.g

- ▶ ouverture du volume chiffré :

- `cryptsetup luksOpen /dev/sdXX maClef`

- ▶ la fenêtre habituelle s'ouvre, utiliser la clef, démonter la clef

# Utilisation

- ▶ Insérer la clef et attendre un peu
- ▶ GNOME (testé avec Lenny)
  - ▶ Dans la fenêtre qui s'ouvre taper la phrase de passe
- ▶ KDE (testé avec Mandriva 2008)
  - ▶ déterminer le volume :  
`dmesg`
  - ▶ ouverture du volume chiffré :  
`cryptsetup luksOpen /dev/sdXX maClef`
- ▶ la fenêtre habituelle s'ouvre, utiliser la clef, démonter la clef

# Utilisation

- ▶ Insérer la clef et attendre un peu
- ▶ GNOME (testé avec Lenny)
  - ▶ Dans la fenêtre qui s'ouvre taper la phrase de passe
- ▶ KDE (testé avec Mandriva 2008)
  - ▶ **déterminer le volume :**  
`dmesg`
  - ▶ ouverture du volume chiffré :  
`cryptsetup luksOpen /dev/sdXX maClef`
  - ▶ la fenêtre habituelle s'ouvre, utiliser la clef, démonter la clef

# Utilisation

- ▶ Insérer la clef et attendre un peu
- ▶ GNOME (testé avec Lenny)
  - ▶ Dans la fenêtre qui s'ouvre taper la phrase de passe
- ▶ KDE (testé avec Mandriva 2008)
  - ▶ déterminer le volume :  
`dmesg`
  - ▶ **ouverture du volume chiffré :**  
`cryptsetup luksOpen /dev/sdXX maClef`
- ▶ la fenêtre habituelle s'ouvre, utiliser la clef, démonter la clef

# Utilisation

- ▶ Insérer la clef et attendre un peu
- ▶ GNOME (testé avec Lenny)
  - ▶ Dans la fenêtre qui s'ouvre taper la phrase de passe
- ▶ KDE (testé avec Mandriva 2008)
  - ▶ déterminer le volume :  
`dmesg`
  - ▶ ouverture du volume chiffré :  
`cryptsetup luksOpen /dev/sdXX maClef`
- ▶ la fenêtre habituelle s'ouvre, utiliser la clef, démonter la clef

## Pour aller plus loin

- ▶ Pour les volumes à monter au démarrage :  
création `/etc/crypttab` :

```
maClef /dev/sdXX none
```

- ▶ Pour partager un volume :

```
cryptsetup luksAddKey /dev/sdXX
```

- ▶ Pour lister les clefs

```
cryptsetup luksDump /dev/sd
```

- ▶ Pour revoquer une clef

```
cryptsetup luksDelKey /dev/sdXX <numéro de clef>
```

- ▶ Il existe un clickoDrôme pour différents OS nommé TrueCrypt ([www.truecrypt.org](http://www.truecrypt.org))



## Pour aller plus loin

- ▶ Pour les volumes à monter au démarrage :  
création `/etc/crypttab` :

```
maClef /dev/sdXX none
```

- ▶ Pour partager un volume :

```
cryptsetup luksAddKey /dev/sdXX
```

- ▶ Pour lister les clefs

```
cryptsetup luksDump /dev/sd
```

- ▶ Pour revoquer une clef

```
cryptsetup luksDelKey /dev/sdXX <numéro de clef>
```

- ▶ Il existe un clickoDrôme pour différents OS nommé TrueCrypt ([www.truecrypt.org](http://www.truecrypt.org))



## Pour aller plus loin

- ▶ Pour les volumes à monter au démarrage :  
création `/etc/crypttab` :

```
maClef /dev/sdXX none
```

- ▶ Pour partager un volume :

```
cryptsetup luksAddKey /dev/sdXX
```

- ▶ Pour lister les clefs

```
cryptsetup luksDump /dev/sd
```

- ▶ Pour revoquer une clef

```
cryptsetup luksDelKey /dev/sdXX <numéro de clef>
```

- ▶ Il existe un clickoDrôme pour différents OS nommé TrueCrypt ([www.truecrypt.org](http://www.truecrypt.org))



## Pour aller plus loin

- ▶ Pour les volumes à monter au démarrage :  
création `/etc/crypttab` :

```
maClef /dev/sdXX none
```

- ▶ Pour partager un volume :

```
cryptsetup luksAddKey /dev/sdXX
```

- ▶ Pour lister les clefs

```
cryptsetup luksDump /dev/sd
```

- ▶ Pour révoquer une clef

```
cryptsetup luksDelKey /dev/sdXX <numéro de clef>
```

- ▶ Il existe un clickoDrôme pour différents OS nommé TrueCrypt ([www.truecrypt.org](http://www.truecrypt.org))



## Pour aller plus loin

- ▶ Pour les volumes à monter au démarrage :  
création `/etc/crypttab` :

```
maClef /dev/sdXX none
```

- ▶ Pour partager un volume :

```
cryptsetup luksAddKey /dev/sdXX
```

- ▶ Pour lister les clefs

```
cryptsetup luksDump /dev/sd
```

- ▶ Pour revoquer une clef

```
cryptsetup luksDelKey /dev/sdXX <numéro de clef>
```

- ▶ Il existe un clickoDrôme pour différents OS nommé TrueCrypt ([www.truecrypt.org](http://www.truecrypt.org))



TP

On essaye ?

