

DE LA RECHERCHE À L'INDUSTRIE



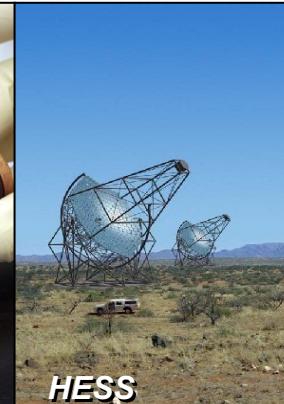
Double Chooz



ALICE



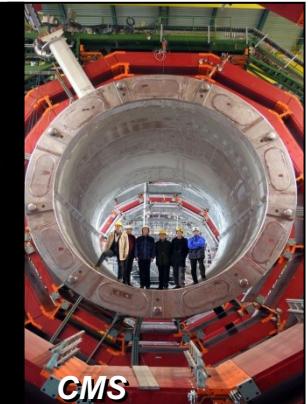
Edelweiss



HESS



Herschel



CMS

Déchiffrer les rayons de l'Univers



P-F Honoré

JII 2021

Chiffrement et déchiffrement sans tête

Chiffrement disque entier ou Full Disk Encryption
=> Bitlocker, Filevault, Luks

Le chiffrement permet de sécuriser nos données : en cas de perte ou de vol, personne ne pourra accéder aux données

- protéger ses informations personnelles
=> KeePass(X)
- garantir la confidentialité des données sensibles
- assurer la réputation du labo, institut...

Attention aux sauvegardes : chiffrées ?

Nécessité au CEA pour tout équipement informatique de conserver HDs, SSDs ... : Keep Your Hard-Drive

=> campagne annuelle de destruction physique

<https://www.youtube.com/watch?v=wdc4tihakys>



Comment appliquer FDE à un portable, à un serveur
- LUKS + clef

Comment appliquer FDE à un portable, à un serveur

- LUKS + clef

➤ KICKSTART : RHEL / CENTOS / ROCKY

```
# Partition clearing information
clearpart --all --initlabel --drives=<%= host_param('install-disk') %>
ignoredisk --only-use=<%= host_param('install-disk') %>
autopart --type=lvm --encrypted --passphrase=<%= host_param('cle-crypto') %> \
--escrowcert= =<%= host_param('URL_of_X.509_certificate') %> --backupperpassword
```

Comment appliquer FDE à un portable, à un serveur - LUKS + clef

➤ KICKSTART : RHEL / CENTOS / ROCKY

```
# Partition clearing information
clearpart --all --initlabel --drives=<%= host_param('install-disk') %>
ignoredisk --only-use=<%= host_param('install-disk') %>
autopart --type=lvm --encrypted --passphrase=<%= host_param('cle-crypto') %> \
--escrowcert= =<%= host_param('URL_of_X.509_certificate') %> --backuppassphrase
```

➤ SEED : DEBIAN / UBUNTU

```
d-i partman-crypto/passphrase password <%= host_param('cle-crypto') %>
d-i partman-crypto/passphrase-again password <%= host_param('cle-crypto') %>
d-i partman-crypto/weak_passphrase boolean true
d-i partman-auto/choose_recipe select boot-crypto
d-i partman-auto-lvm/guided_size string 68GB
d-i partman-auto-lvm/new_vg_name string crypt
d-i partman-auto/expert_recipe string boot-crypto :: \
    32 32 32 free \$primary{ } \$bios_boot{ } method{ biosgrub } . \
    40 50 100 fat16 \$primary{ } \$bootable{ } method{ efi } format{ } filesystem{ fat16 } . \
#      256 512 512 ext4 \$primary{ } \$bootable{ } method{ format } format{ } use_filesystem{ } filesystem{ \
ext4 } mountpoint{ /boot } . \
    2048 2048 2048 ext4 \$primary{ } \$bootable{ } method{ format } format{ } use_filesystem{ } filesystem{ \
ext4 } mountpoint{ /boot } . \
#
#      2072 3072 3072 ext4 $lvmok{ } lv_name{ root } \
#      4096 5120 5120 ext4 $lvmok{ } lv_name{ root } \
    8192 11024 11024 ext4 $lvmok{ } lv_name{ root } \
    in_vg { crypt } method{ format } format{ } \
    use_filesystem{ } filesystem{ ext4 } mountpoint{ / } \
. \
```

Settings	
General	
System Information	
Battery Information	
Boot Sequence	
UEFI Boot Path Security	
Date/Time	
System Configuration	
Video	
Security	
Admin Password	
System Password	
Password Configuration	
Password Bypass	
Password Change	
UEFI Capsule Firmware Updates	
TPM 2.0 Security	
Absolute®	
OROM Keyboard Access	
Admin Setup Lockout	
Master Password Lockout	
SMM Security Mitigation	
Secure Boot	
Intel® Software Guard Extensions™	
Performance	
Power Management	
POST Behavior	
Virtualization Support	
Wireless	
Maintenance	
System Logs	
About	
SupportAssist System Resolution	

TPM On Clear

Attestation Enable Key Storage Enable

PPI Bypass for Clear Command SHA-256

Disabled Enabled

TPM On :
This option lets you control whether the Trusted Platform Module (TPM) is visible to the operating system.
NOTE: Disabling this option does not change any settings you have made to the TPM, nor does it delete or change any information or keys you may have stored in the TPM. Changes to this setting take effect immediately.

Clear :
This setting clears the TPM owner information, and the TPM is "Enabled" after the Clear. Changes to this setting take effect in the TPM upon exit from the BIOS setup menu.

PPI Bypass for Enable Commands :
This option controls the TPM Physical Presence Interface (PPI). When enabled, this setting will allow the OS to skip BIOS PPI user prompts when issuing TPM PPI enable and activate commands (# 1,3,6,8,10). See TCG PPI specification for more details. Changes to this setting take effect immediately.

PPI Bypass for Disable Commands :
This option controls the TPM Physical Presence Interface (PPI). When enabled, this setting will allow the OS to skip BIOS PPI user prompts when issuing TPM PPI Disable and Deactivate commands (# 2,4,7,9,11). See TCG PPI specification for more details. Changes to this setting take effect immediately.

PPI Bypass for Clear Command:
This option controls the TPM Physical Presence Interface (PPI). When enabled, this setting will allow the OS

- LUKS + TPM2

CONDITION = ENVIRONNEMENT SÉCURISÉ

➤ SYSTEMD >=248 : ARCHLINUX, UBUNTU 22.04 OU RHEL 9

```
systemd-cryptenroll /dev/nvme0n1p2 --tpm2-device=auto --tpm2-pcrs=7
```

- LUKS + TPM2

CONDITION = ENVIRONNEMENT SÉCURISÉ

- SYSTEMD >=248 : ARCHLINUX, UBUNTU 22.04 OU RHEL 9

```
systemd-cryptenroll /dev/nvme0n1p2 --tpm2-device=auto --tpm2-pcrs=7
```

- CLEVIS

```
sudo apt install -y clevis clevis-luks clevis-tpm2 clevis-initramfs
sudo clevis luks bind -d /dev/mmcblk0p2 tpm2 '{"pcr_ids":"7"}' »
sudo update-initramfs -u
```

- LUKS + TPM2

CONDITION = ENVIRONNEMENT SÉCURISÉ

- SYSTEMD >=248 : ARCHLINUX, UBUNTU 22.04 OU RHEL 9

```
systemd-cryptenroll /dev/nvme0n1p2 --tpm2-device=auto --tpm2-pcrs=7
```

- CLEVIS

```
sudo apt install -y clevis clevis-luks clevis-tpm2 clevis-initramfs
sudo clevis luks bind -d /dev/mmcblk0p2 tpm2 '{"pcr_ids":"7"}' »
sudo update-initramfs -u
```

QUE CONTIENT LE NOUVEL INITRAMFS ?

```
honore@irfupcz49:~$ sudo lsinitramfs /boot/initrd.img-5.13.0-19-generic |grep -E 'cryptsetup|tpm2'
usr/bin/clevis-decrypt-tpm2
usr/bin/tpm2
usr/bin/tpm2_createprimary
usr/bin/tpm2_load
usr/bin/tpm2_unseal
usr/lib/cryptsetup
usr/lib/cryptsetup/askpass
usr/lib/cryptsetup/functions
usr/lib/modules/5.13.0-19-generic/kernel/crypto/asymmetric_keys/asym_tpm.ko
usr/lib/modules/5.13.0-19-generic/kernel/crypto/asymmetric_keys/tpm_key_parser.ko
usr/lib/x86_64-linux-gnu/libcryptsetup.so.12
usr/lib/x86_64-linux-gnu/libcryptsetup.so.12.6.0
usr/sbin/cryptsetup
honore@irfupcz49:~$
```

EN PARALLÈLE DE ASKPASS

DECHIFFREMENT TPM2 SANS TÊTE



- LUKS + NETWORK-BOUND DISK ENCRYPTION
CONDITION = RÉSEAU SÉCURISÉ



- LUKS + NETWORK-BOUND DISK ENCRYPTION
CONDITION = RÉSEAU SÉCURISÉ



➤ TANG

```
# CentOS
dnf install -y tang
# Debian
apt install -y tang
# Enable the tangd.socket
systemctl enable tangd.socket
```

- LUKS + NETWORK-BOUND DISK ENCRYPTION

CONDITION = RÉSEAU SÉCURISÉ



➤ TANG

```
# CentOS
dnf install -y tang
# Debian
apt install -y tang
# Enable the tangd.socket
systemctl enable tangd.socket
```

➤ CLEVIS

```
[honore@centos7 ~]$ sudo yum install clevis-dracut clevis-systemd clevis-luks
[honore@centos7 ~]$ sudo clevis luks bind -d /dev/sda2 tang '{ "url": "http://192.168.56.4"}'
```

- LUKS + NETWORK-BOUND DISK ENCRYPTION

CONDITION = RÉSEAU SÉCURISÉ



➤ TANG

```
# CentOS
dnf install -y tang
# Debian
apt install -y tang
# Enable the tangd.socket
systemctl enable tangd.socket
```

➤ CLEVIS

```
[honore@centos7 ~]$ sudo yum install clevis-dracut clevis-systemd clevis-luks
[honore@centos7 ~]$ sudo clevis luks bind -d /dev/sda2 tang '{ "url": "http://192.168.56.4"}'
The advertisement contains the following signing keys:
```

```
nMHMvOaGlTxhbofEfqAPvoqlnUY
```

```
Do you wish to trust these keys? [ynYN] Y
You are about to initialize a LUKS device for metadata storage.
Attempting to initialize it may result in data loss if data was
already written into the LUKS header gap in a different format.
A backup is advised before initialization is performed.
```

```
Do you wish to initialize /dev/sda2? [yn] y
```

```
Enter existing LUKS password:
```

```
[honore@centos7 ~]$ sudo dracut -f --kernel-cmdline ifname=enp0s8:08:00:27:1a:d5:e4'
[honore@centos7 ~]$ sudo lsinitrd /boot/initramfs-3.10.0-1160.e17.x86_64.img |grep -E 'clevis-decrypt-tang'
-rwxr-xr-x 1 root      root          2712 Oct 30  2018 usr/bin/clevis-decrypt-tang
[honore@centos7 ~]$
```

DE-DÉCHIFFREMENT TPM2

```
honore@irfupcz49:~$ sudo clevis luks bind -d /dev/nvme0n1p3 tpm2 '{"pcrs_ids":"01,2,3,4,5,6,7,8"}'  
Enter existing LUKS password:  
Warning: Value 512 is outside of the allowed entropy range, adjusting it.  
honore@irfupcz49:~$ sudo cryptsetup luksDump /dev/nvme0n1p3|grep -B1 Key:  
 0: luks2  
      Key:      512 bits  
--  
 1: luks2  
      Key:      512 bits  
--  
 2: luks2  
      Key:      512 bits
```

DE-DÉCHIFFREMENT TPM2

```
honore@irfupcz49:~$ sudo clevis luks bind -d /dev/nvme0n1p3 tpm2 '{"pcrs_ids":"01,2,3,4,5,6,7,8"}'  
Enter existing LUKS password:  
Warning: Value 512 is outside of the allowed entropy range, adjusting it.  
honore@irfupcz49:~$ sudo cryptsetup luksDump /dev/nvme0n1p3|grep -B1 Key:  
 0: luks2  
      Key:      512 bits  
--  
 1: luks2  
      Key:      512 bits  
--  
 2: luks2  
      Key:      512 bits  
honore@irfupcz49:~$ sudo reboot
```

DE-DÉCHIFFREMENT TPM2

```
honore@irfupcz49:~$ sudo clevis luks bind -d /dev/nvme0n1p3 tpm2 '{"pcrs_ids":"01,2,3,4,5,6,7,8"}'
Enter existing LUKS password:
Warning: Value 512 is outside of the allowed entropy range, adjusting it.
honore@irfupcz49:~$ sudo cryptsetup luksDump /dev/nvme0n1p3|grep -B1 Key:
 0: luks2
      Key:      512 bits
--
 1: luks2
      Key:      512 bits
--
 2: luks2
      Key:      512 bits
honore@irfupcz49:~$ sudo reboot

honore@irfupcz49:~$ sudo tpm2_clear -T device:/dev/tpm0
honore@irfupcz49:~$ sudo cryptsetup luksKillSlot /dev/disk/by-uuid/cb2a85e9-eb87-45c9-b18f-4df8b54a7d7f 2
Enter any remaining passphrase:
honore@irfupcz49:~$ sudo cryptsetup luksDump /dev/disk/by-uuid/cb2a85e9-eb87-45c9-b18f-4df8b54a7d7f |grep -B1
Key:
 0: luks2
      Key:      512 bits
--
 1: luks2
      Key:      512 bits
honore@irfupcz49:~$
```



Commissariat à l'énergie atomique et aux énergies alternatives
Centre de Saclay | 91191 Gif-sur-Yvette Cedex

Etablissement public à caractère industriel et commercial | R.C.S Paris B 775 685 019

Direction de la Recherche Fondamentale
Institut de recherche
sur les lois fondamentales de l'Univers
Service