Linux Sicuro sin dal Boot

Cosa sono Secure Boot, Measured Boot e TPM

/usr/bin/whoami

Daniele Barcella

@kowalski7cc - https://www.linkedin.com/in/daniele-barcella-it/

Linux dal 2006, BgLUG dal ???, unixMiB dal 2015

EUCIP IT Administrator dal 2014

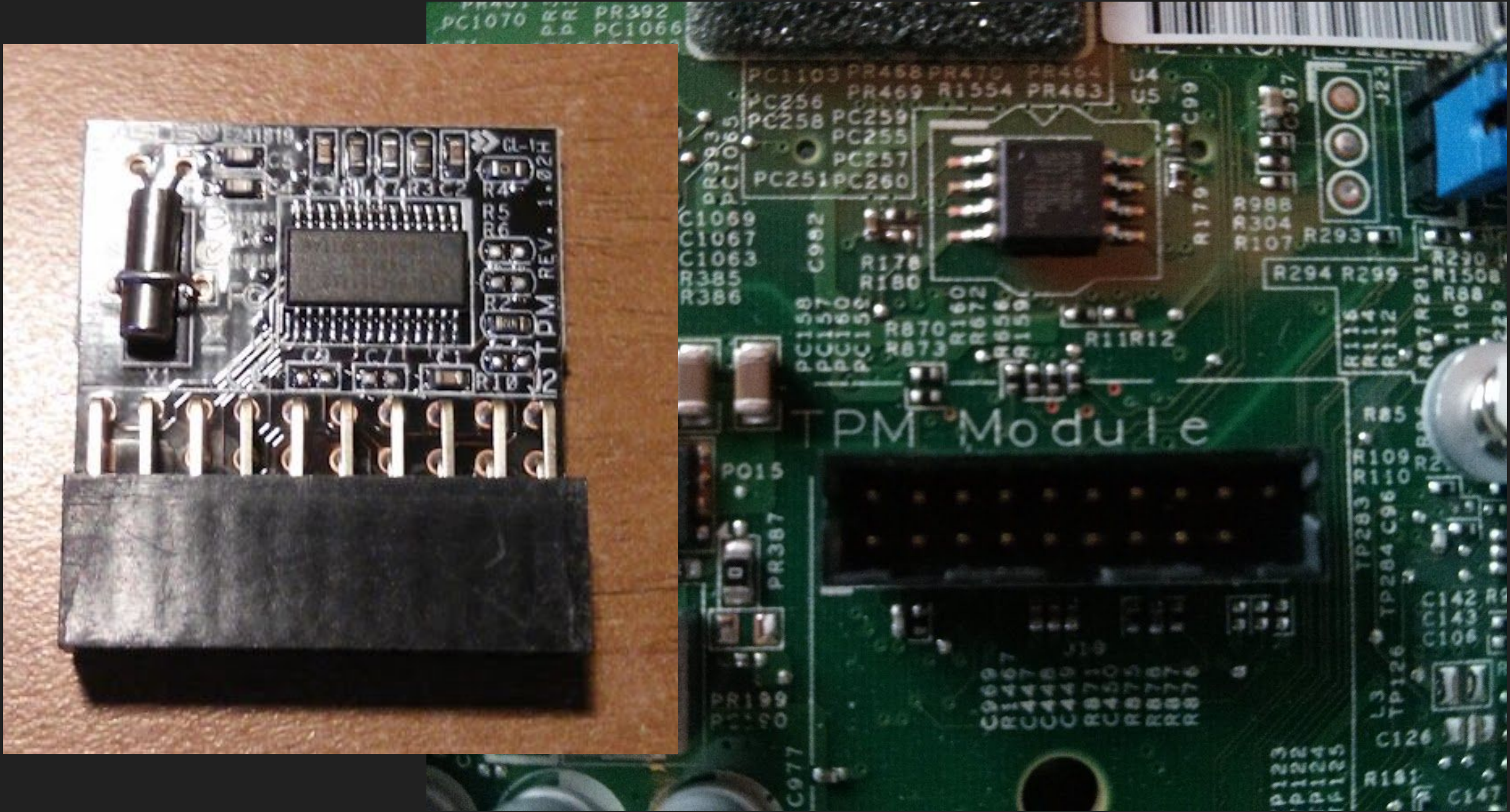
Consulente e Istruttore Red Hat in EXTRAORDY

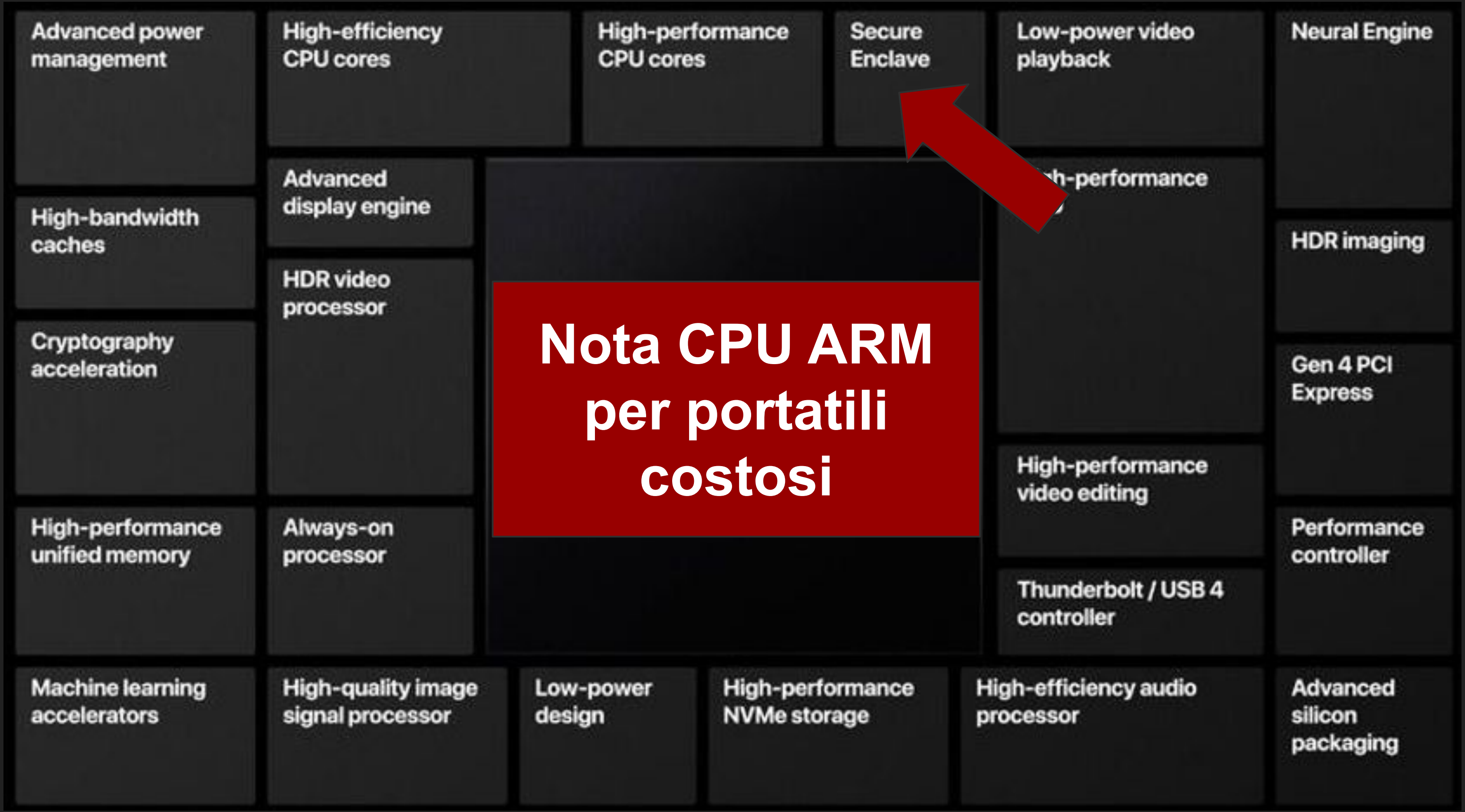
- Red Hat Certified Enterprise Application Developer dal 2021
- Red Hat Certified System Administrator dal 2022
- Red Hat Certified Engineer e Red Hat Certified Instructor dal 2023
- // TODO: espandere la lista

Cosa vedremo oggi?

TPM: Trusted Platform Module

Blocco hardware?


TPM REV. 1.02H
CL-1H
J2
TPM Module
J19



Advanced power management

High-bandwidth caches

Cryptography acceleration

High-performance unified memory

Machine learning accelerators

High-efficiency CPU cores

Advanced display engine

HDR video processor

Always-on processor

High-quality image signal processor

High-performance CPU cores

Low-power design

High-performance NVMe storage

Secure Enclave

Low-power video playback

h-performance

High-performance video editing

Thunderbolt / USB 4 controller

High-efficiency audio processor

Neural Engine

HDR imaging

Gen 4 PCI Express

Performance controller

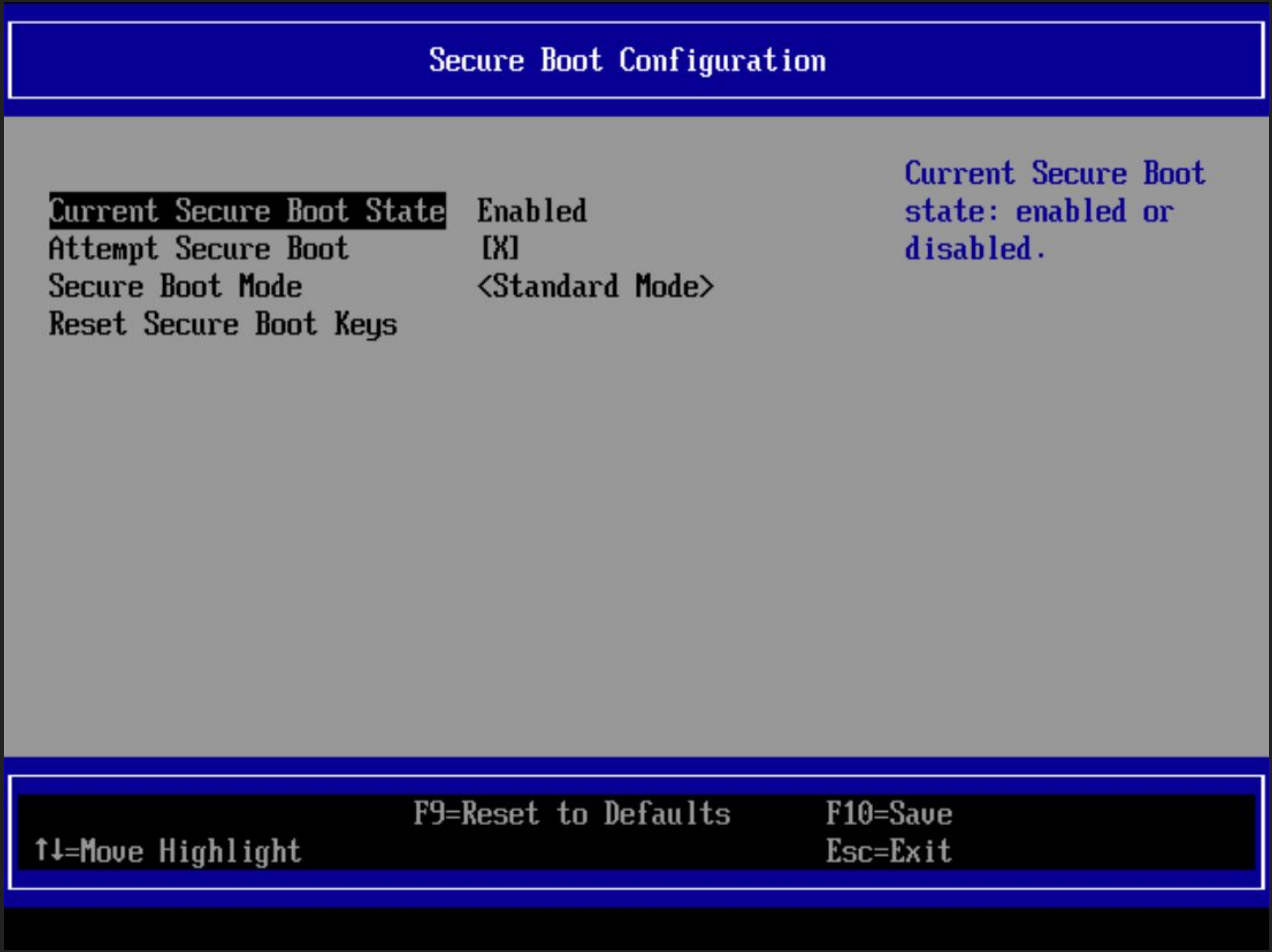
Advanced silicon packaging

Nota CPU ARM per portatili costosi

TPM: just good at math?

- Hardware o software (dTPM, hwTPM, swTPM, fwTPM, vTPM...)
- TPM 1.2 e TPM 2.0
- LCP o SPI bus
  - ISA BUS coi baffi
- Cryptographic processor
  - Random Number Generator
  - Generatore di chiavi
  - Encryption-Decryption engine (RSA, ECC in TPM 2.0)
  - HASH engine (SHA-1 e SHA-256 in TPM 2.0)
- Secret storage
  - Storage Root Key (SRK)
  - Endorsement Key (EK)
  - Platform Configuration Registries (PCR) ←
  - Attestation Identity keys (AIK)
  - Storage Keys

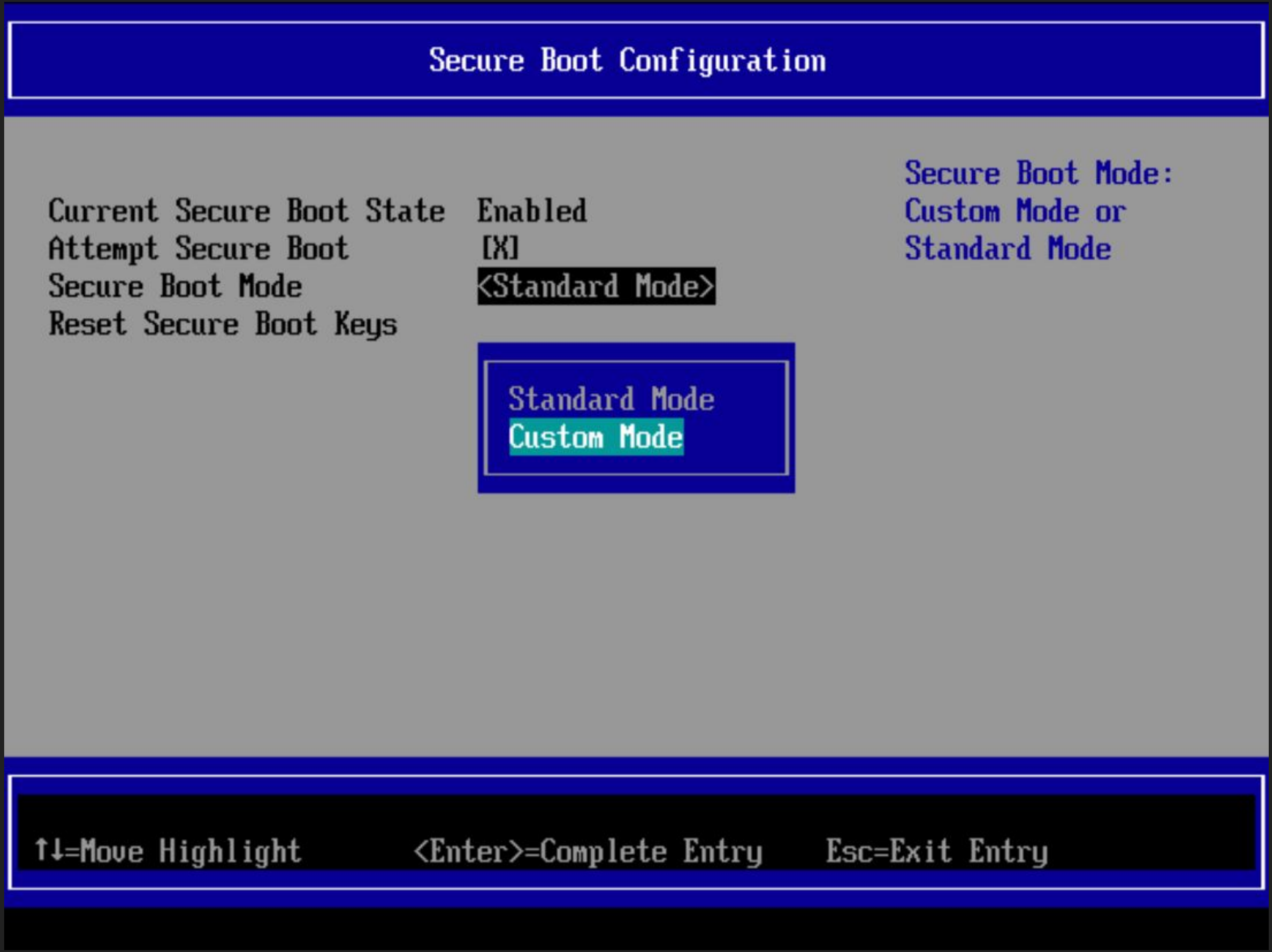
Secure Boot
Dittatura digitale?



Secure Boot Configuration

```
Current Secure Boot State      Enabled
Attempt Secure Boot            [X]
Secure Boot Mode               <Standard Mode>
Reset Secure Boot Keys
```

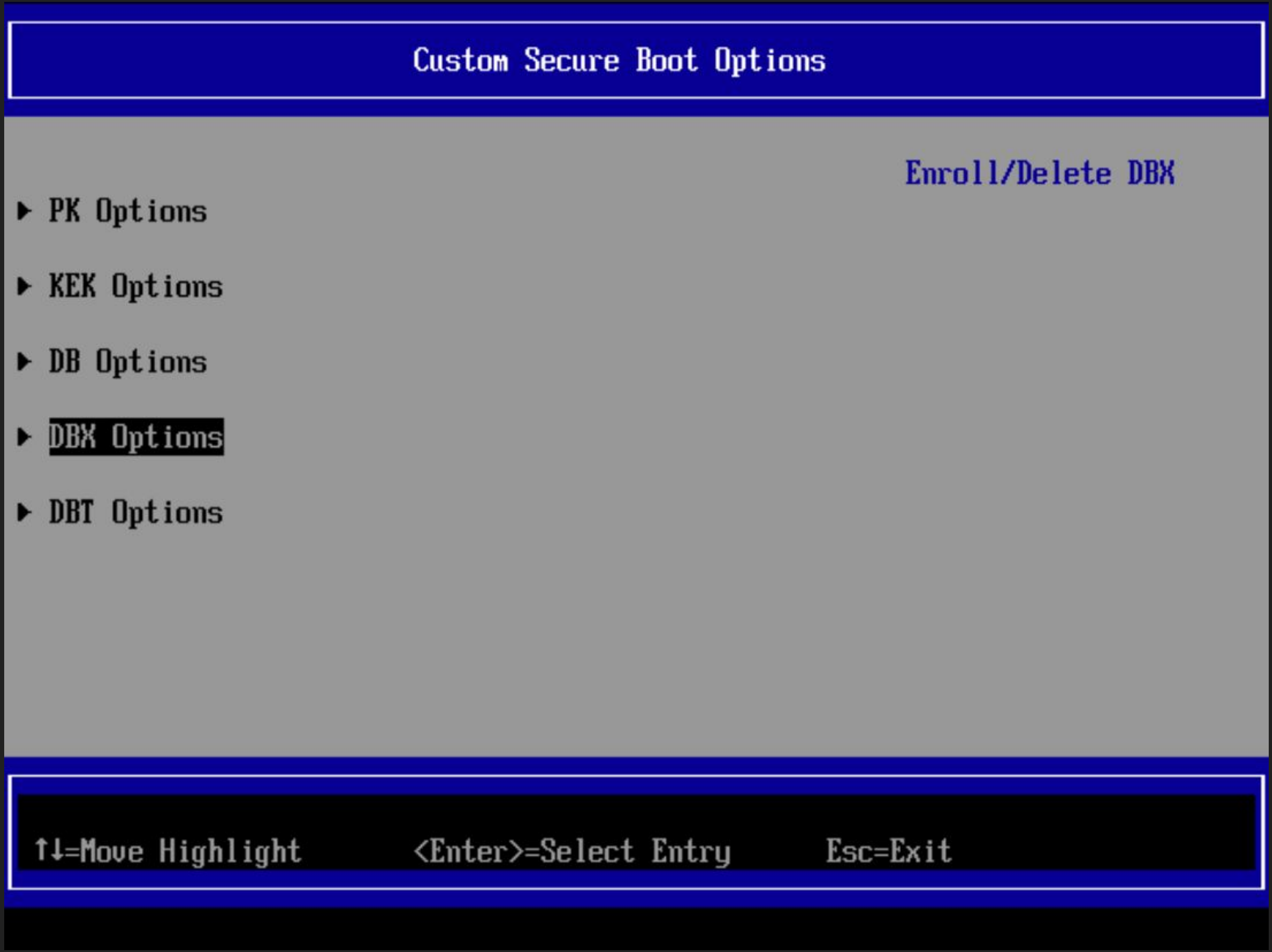
Current Secure Boot state: enabled or disabled.



Secure Boot Configuration

Current Secure Boot State Enabled
Attempt Secure Boot [X]
Secure Boot Mode <Standard Mode>
Reset Secure Boot Keys

Secure Boot Mode: Custom Mode or Standard Mode



Custom Secure Boot Options

Enroll/Delete DBX

▶ PK Options

▶ KEK Options

▶ DB Options

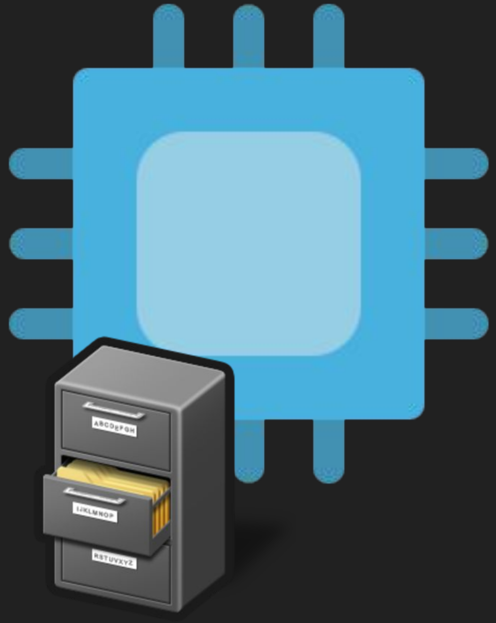
▶ DBX Options

▶ DBT Options

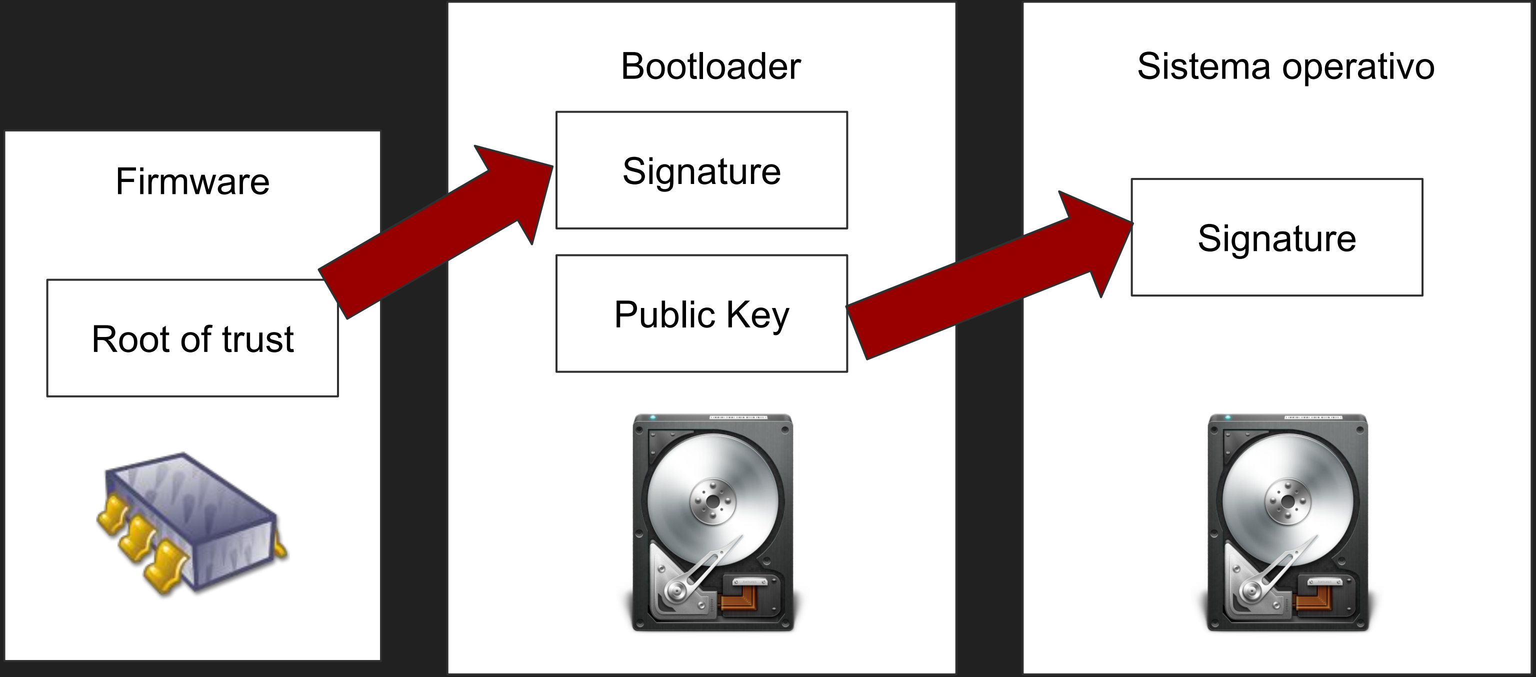
↑↓=Move Highlight <Enter>=Select Entry Esc=Exit

Secure Boot: un modo per impedire l’avvio di sistemi (binari EFI) non autorizzati mediante “firma digitale”

CPU: quando posso eseguire codice?



SecureBoot: Chain of trust al boot



Firmware

Root of trust

Bootloader

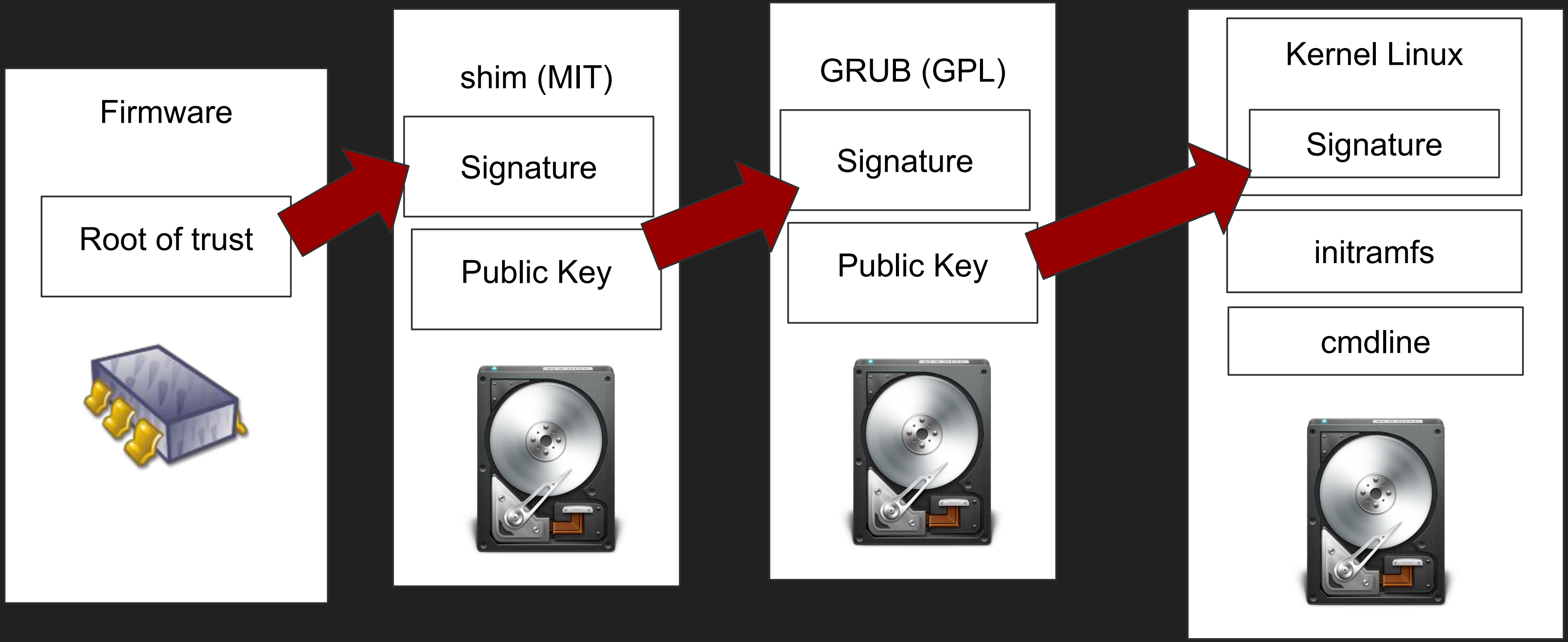
Signature

Public Key

Sistema operativo

Signature

Secure Boot su Linux



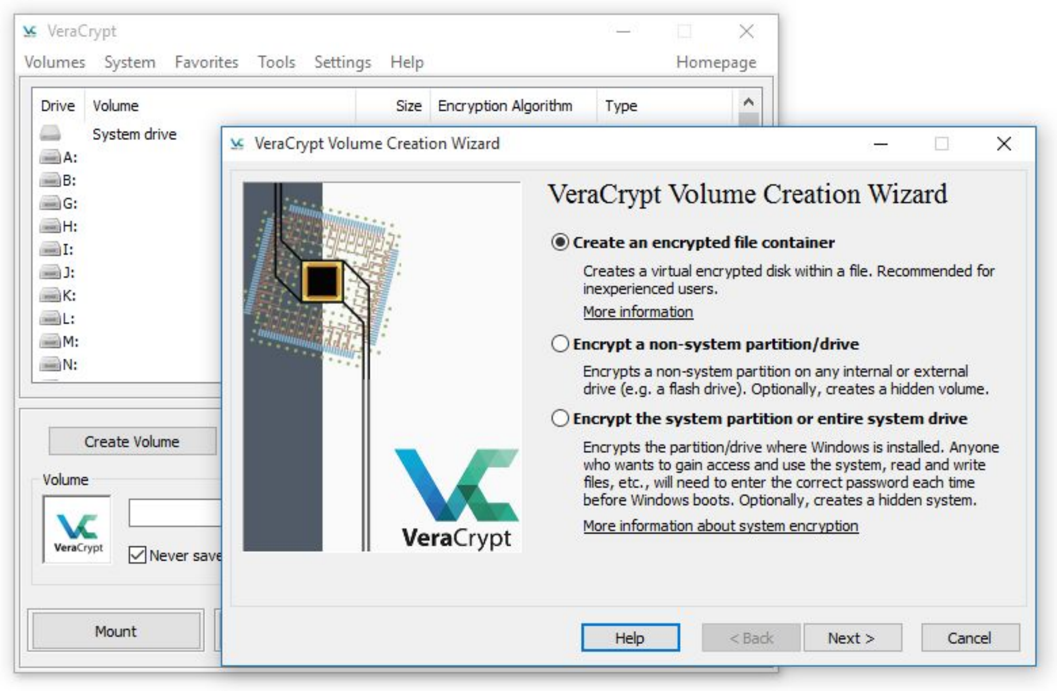
SecureBoot: davvero sicuro?

https://thehackernews.com/2016/08/uefi-secure-boot-hack.html

https://habr.com/en/articles/446238/

- Exploiting signed bootloaders to circumvent UEFI Secure Boot
- Microsoft Accidentally Leaks Backdoor Keys to Bypass UEFI Secure Boot
- Mantenere aggiornato il DB delle chiavi revocate nel firmware
- Installare solamente le chiavi strettamente necessarie

Full Disk Encryption
vs.
File Encryption



Drive	Volume	Size	Encryption Algorithm	Type
	System drive			
A:				
B:				
G:				
H:				
I:				
J:				
K:				
L:				
M:				
N:				

Volume

☑ Never save

VeraCrypt Volume Creation Wizard

VeraCrypt Volume Creation Wizard

● **Create an encrypted file container**

Creates a virtual encrypted disk within a file. Recommended for inexperienced users.

More information

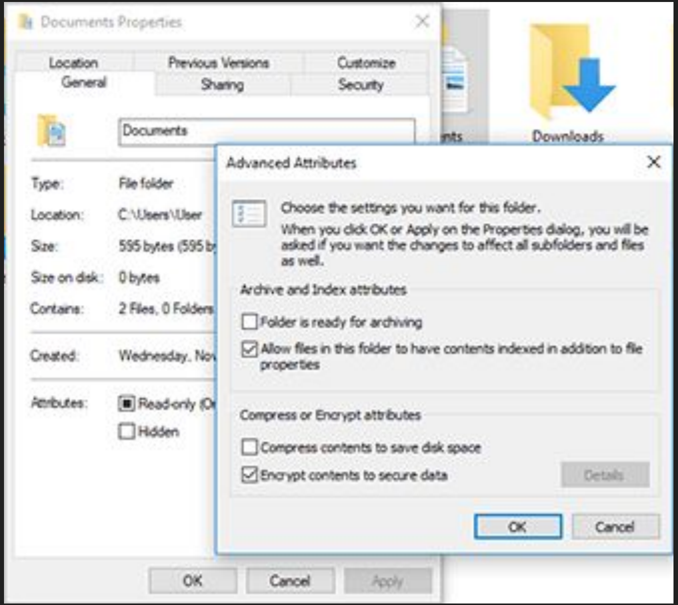
○ **Encrypt a non-system partition/drive**

Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.

○ **Encrypt the system partition or entire system drive**

Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.

More information about system encryption



Documents

Type: File folder

Location: C:\Users\User

Size: 595 bytes (595 b

Size on disk: 0 bytes

Contains: 2 Files, 0 Folders

Created: Wednesday, Nov

Attributes: ■ Read-only (O
□ Hidden

Advanced Attributes

Choose the settings you want for this folder.

When you click OK or Apply on the Properties dialog, you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

□ Folder is ready for archiving

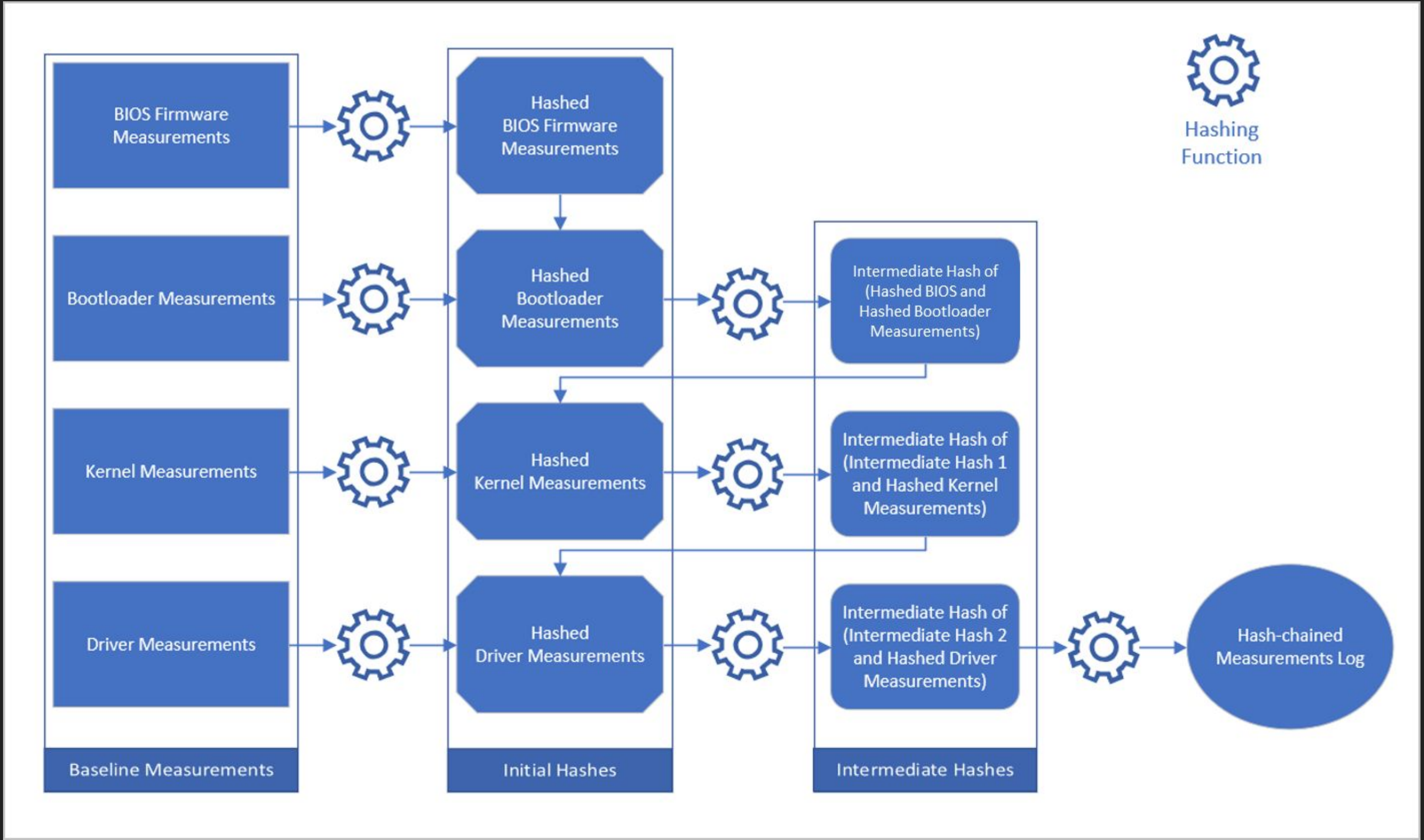
☑ Allow files in this folder to have contents indexed in addition to file properties

Compress or Encrypt attributes

□ Compress contents to save disk space

☑ Encrypt contents to secure data

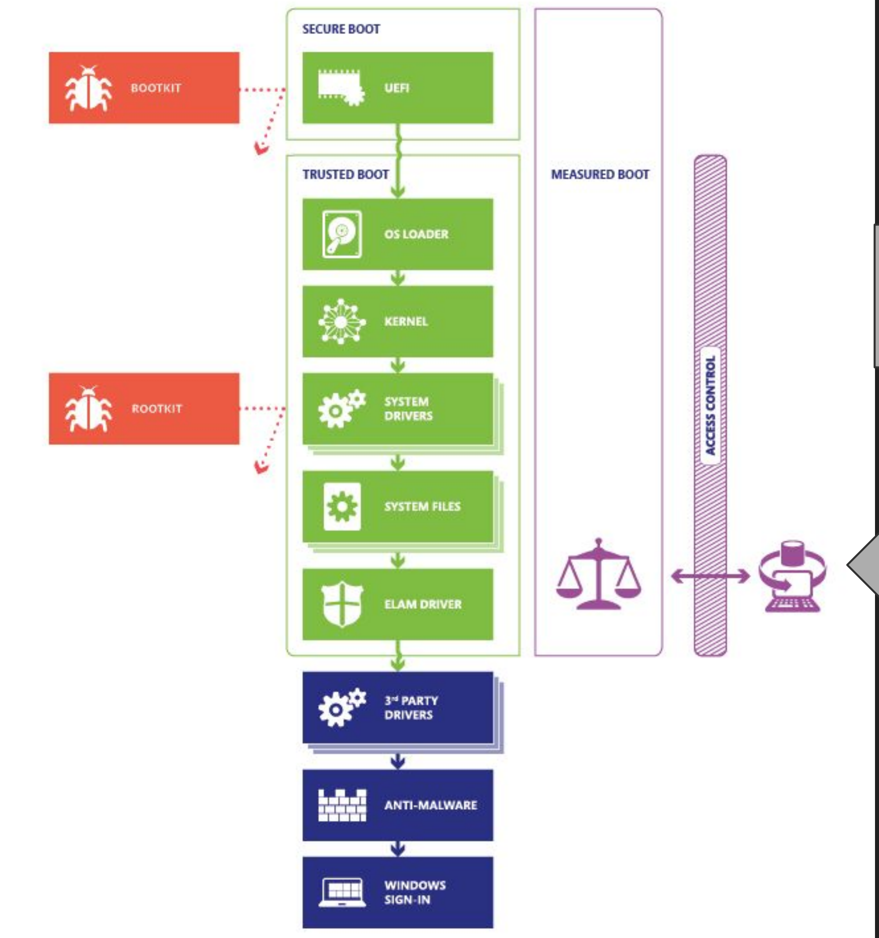
Measured Boot ????


Hashing Function
BIOS Firmware Measurements
Bootloader Measurements
Kernel Measurements
Driver Measurements
Baseline Measurements
Hashed BIOS Firmware Measurements
Hashed Bootloader Measurements
Hashed Kernel Measurements
Hashed Driver Measurements
Initial Hashes
Intermediate Hash of (Hashed BIOS and Hashed Bootloader Measurements)
Intermediate Hash of (Intermediate Hash 1 and Hashed Kernel Measurements)
Intermediate Hash of (Intermediate Hash 2 and Hashed Driver Measurements)
Intermediate Hashes
Hash-chained Measurements Log

https://learn.microsoft.com/en-us/azure/security/fundamentals/measured-boot-host-attestation#measured-boot

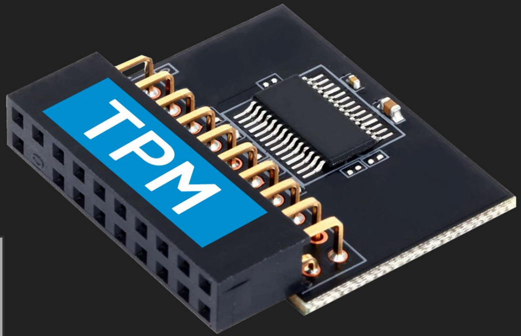
Dove e come teniamo traccia delle misure?

TPM PCRs



PCRs

Disk Encryption Key



https://learn.microsoft.com/en-us/windows/security/operating-system-security/system-security/secure-the-windows-10-boot-process

PCR ID	Description
0	Firmware
1	Firmware configuration
2	Option ROMs
3	Option ROMs configuration
4	MBR
5	MBR Configuration
6	State transition
7	Platform-specific
8 - 15	Operating System reserved
16	Debug
23	Applications

Measured boot: Attacchi coldboot?

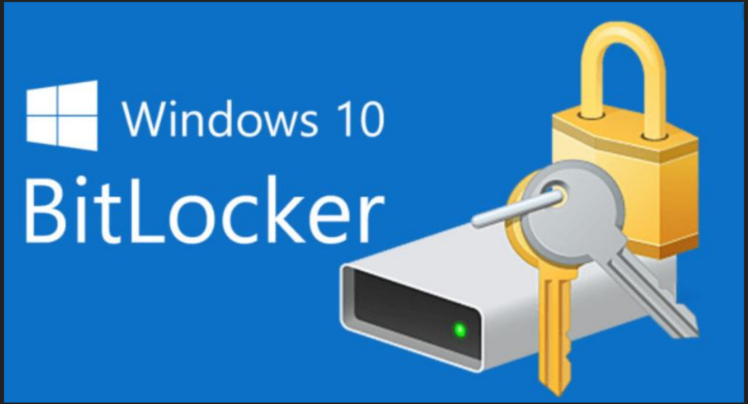
https://blog.f-secure.com/cold-boot-attacks/

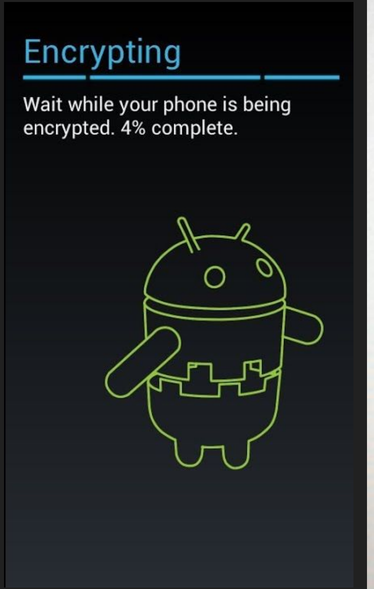
https://www.zdnet.com/article/new-bitlocker-attack-puts-laptops-storing-sensitive-data-at-risk/

https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/bitlocker-countermeasures

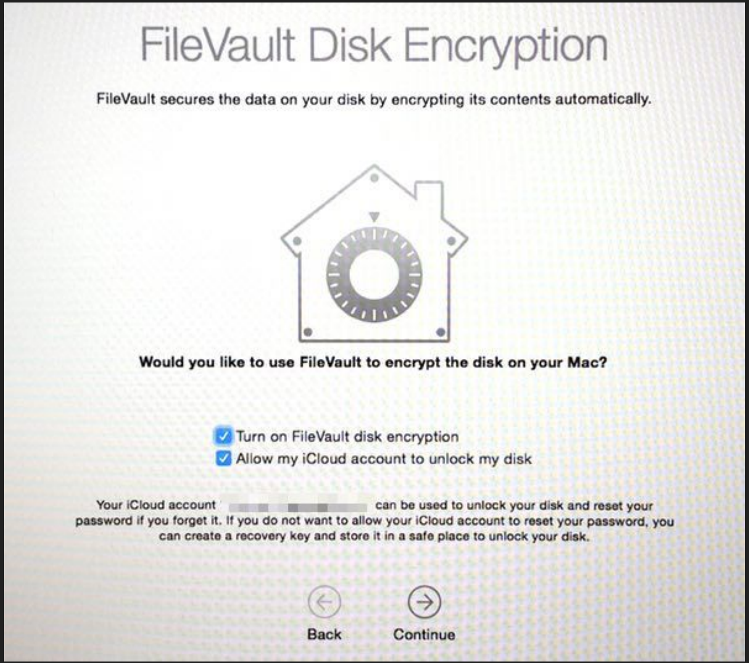
- Evil maid attacks
  - The Chilling Reality of Cold Boot Attacks
    - Estrazione chiave da RAM
      - RAM encryption
  - New BitLocker attack puts laptops storing sensitive data at risk
    - Sniffing/Reply attack su BUS LCP
- BitLocker Countermeasures
  - TPM + PIN
  - User Profile encryption

Quali sono le soluzioni nei vari sistemi operativi?




Encrypting

Wait while your phone is being encrypted. 4% complete.

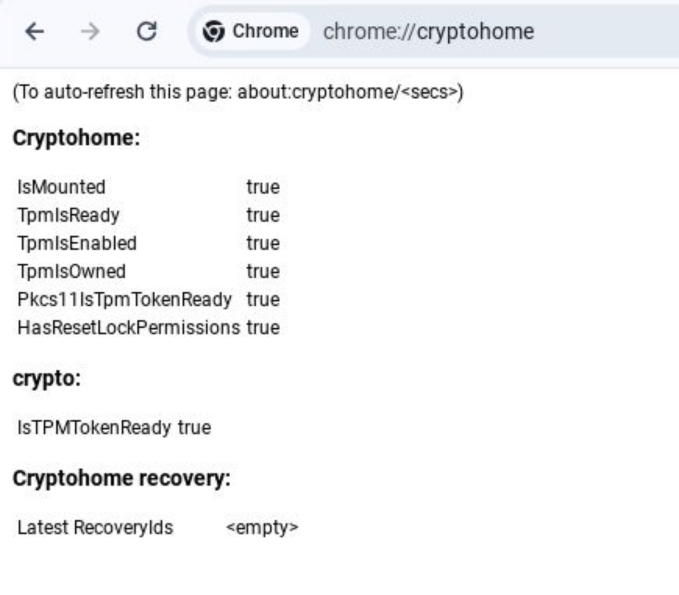

FileVault Disk Encryption

FileVault secures the data on your disk by encrypting its contents automatically.

Would you like to use FileVault to encrypt the disk on your Mac?

☑ Turn on FileVault disk encryption
☑ Allow my iCloud account to unlock my disk

Your iCloud account [redacted] can be used to unlock your disk and reset your password if you forget it. If you do not want to allow your iCloud account to reset your password, you can create a recovery key and store it in a safe place to unlock your disk.



chrome://cryptohome

(To auto-refresh this page: about:cryptohome/<secs>)

Cryptohome:

```
IsMounted               true
TpmIsReady              true
TpmIsEnabled            true
TpmIsOwned              true
Pkcs11IsTpmTokenReady   true
HasResetLockPermissions true
```

crypto:

```
IsTPMTokenReady true
```

Cryptohome recovery:

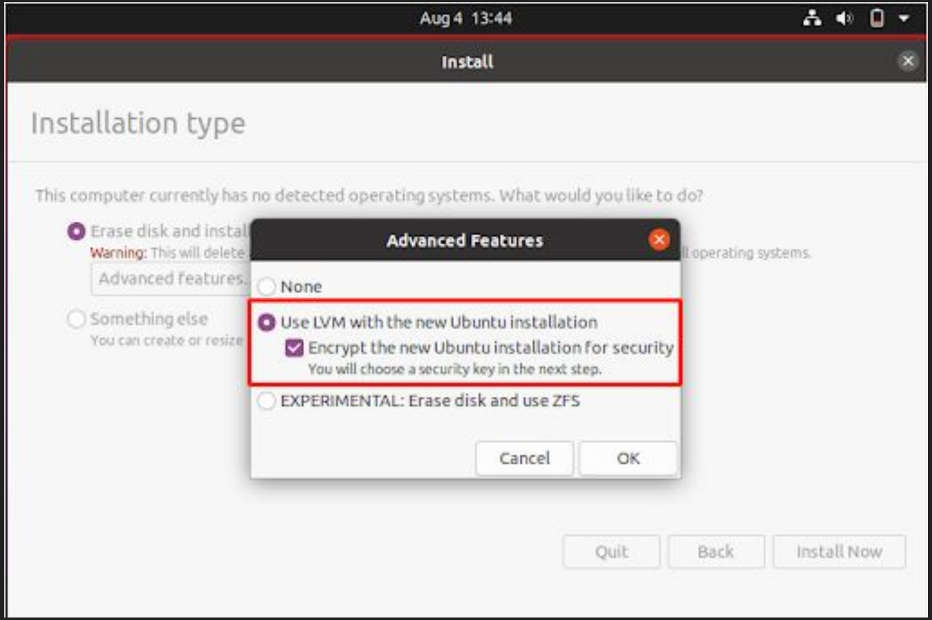
```
Latest RecoveryIds      <empty>
```

Come replichiamo su una distribuzione Linux?

Full Disk Encryption

Come configuro LUKS

- Configurazione durante l’installazione



Aug 4 13:44

Install

Installation type

This computer currently has no detected operating systems. What would you like to do?

● Erase disk and instal

Warning: This will delete … ll operating systems.

Advanced features…

○ Something else

You can create or resize

Advanced Features

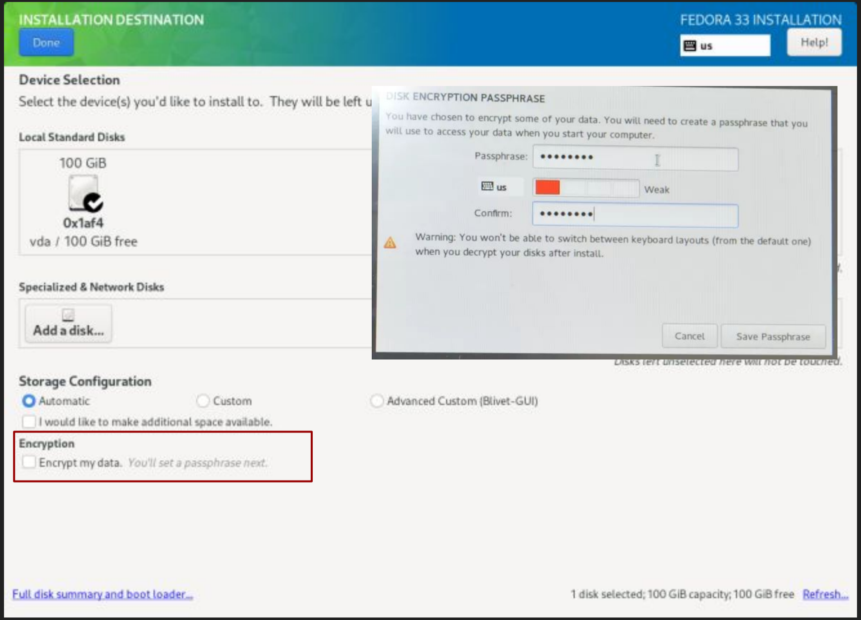
○ None

● Use LVM with the new Ubuntu installation

☑ Encrypt the new Ubuntu installation for security

You will choose a security key in the next step.

○ EXPERIMENTAL: Erase disk and use ZFS



INSTALLATION DESTINATION

FEDORA 33 INSTALLATION

Device Selection

Select the device(s) you'd like to install to. They will be left u

Local Standard Disks

100 GiB

0x1af4

vda / 100 GiB free

Specialized & Network Disks

DISK ENCRYPTION PASSPHRASE

You have chosen to encrypt some of your data. You will need to create a passphrase that you will use to access your data when you start your computer.

Passphrase: ••••••••

us Weak

Confirm: ••••••••

Warning: You won't be able to switch between keyboard layouts (from the default one) when you decrypt your disks after install.

Disks left unselected here will not be touched.

Storage Configuration

● Automatic ○ Custom ○ Advanced Custom (Blivet-GUI)

□ I would like to make additional space available.

Encryption

□ Encrypt my data. *You'll set a passphrase next.*

1 disk selected; 100 GiB capacity; 100 GiB free

Come configuro LUKS

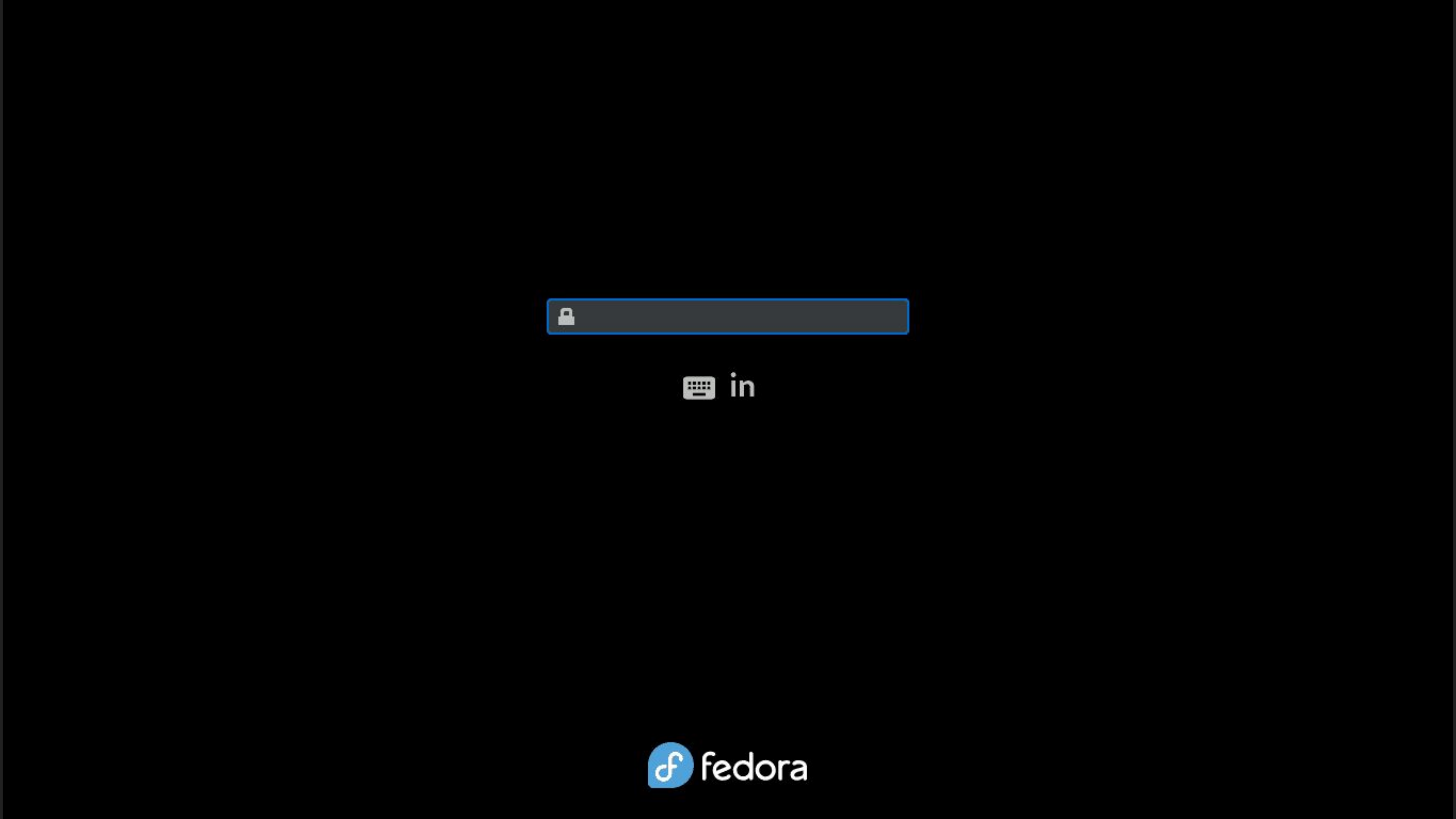
- Configurazione durante l’installazione

```
[kowalski7cc@Kaos ~]$ lsblk
NAME                                          MAJ:MIN RM   SIZE RO TYPE  MOUNTPOINT
nvme0n1                                       259:0    0   477G  0 disk
├─nvme0n1p1                                   259:1    0   600M  0 part  /boot/efi
├─nvme0n1p2                                   259:2    0     1G  0 part  /boot
└─nvme0n1p3                                   259:3    0 475,4G  0 part
  └─luks-xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx 253:0    0 475,3G  0 crypt
    ├─fedora_localhost--live-root             253:1    0    70G  0 lvm   /
    ├─fedora_localhost--live-swap             253:2    0   7,8G  0 lvm   [SWAP]
    └─fedora_localhost--live-home             253:3    0 397,6G  0 lvm   /home
```

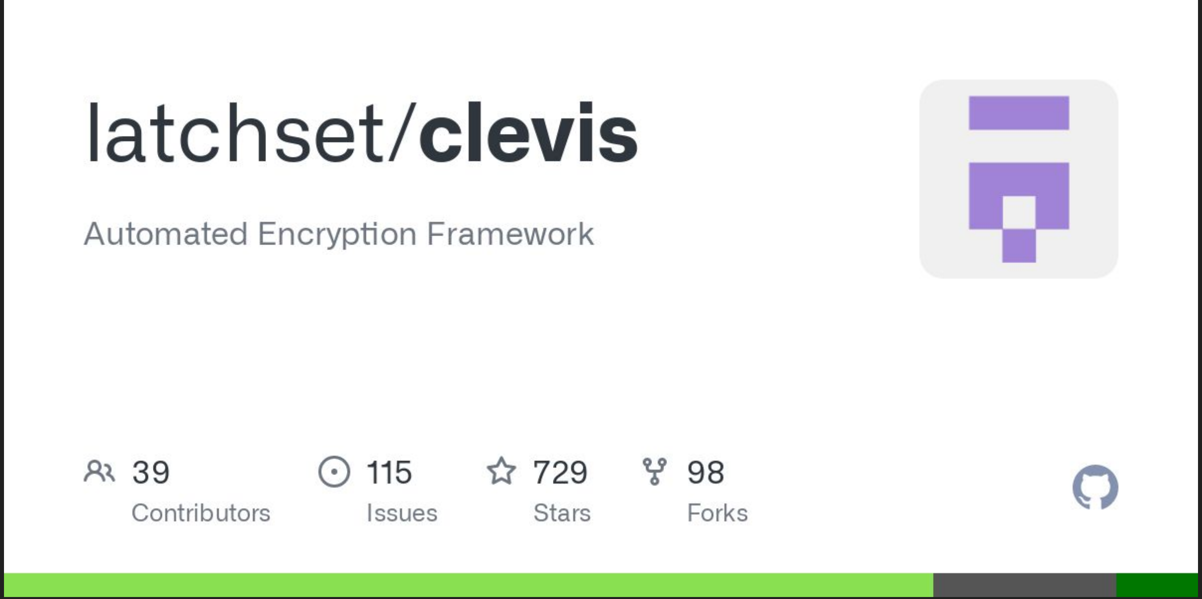
Come configuro LUKS

- Configurazione durante l’installazione

```
[kowalski7cc@Kaos ~]$ sudo cryptsetup luksDump /dev/nvme0n1p3
[sudo] password di kowalski7cc:
LUKS header information
Version:        2
Epoch:          3
Metadata area:  16384 [bytes]
Keyslots area:  16744448 [bytes]
UUID:           xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Label:          (no label)
Subsystem:      (no subsystem)
Flags:          (no flags)
```



in
fedora



latchset/**clevis**

Automated Encryption Framework

39 Contributors

115 Issues

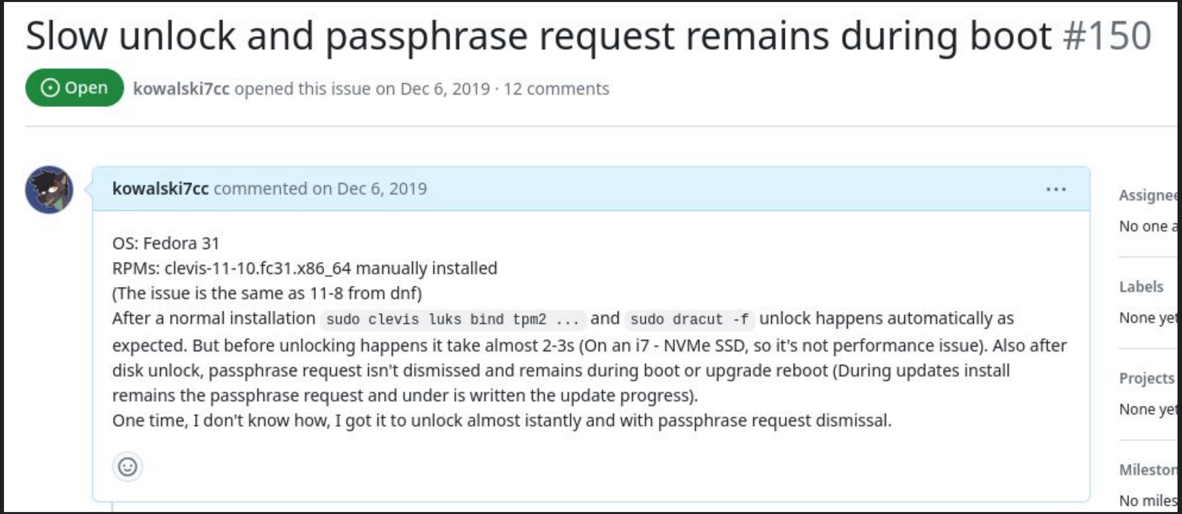
729 Stars

98 Forks

https://github.com/latchset/clevis

Unlock automatico con Clevis

```
[kowalski7cc@Kaos ~]$ sudo dnf install clevis clevis-luks clevis-dracut \
clevis-udisks2 clevis-systemd

[kowalski7cc@Kaos ~]$ sudo clevis luks bind -d /dev/nvme0n1p3 tpm2 \
'{"pcr_ids":"0,1,2,3,4,5,6,7"}'

[kowalski7cc@Kaos ~]$ sudo cryptsetup luksDump /dev/nvme0n1p3
[sudo] password di kowalski7cc:
LUKS header information
Version:        2
Epoch:          7
...
Tokens:
  0: clevis
  Keyslot:  1
...
```

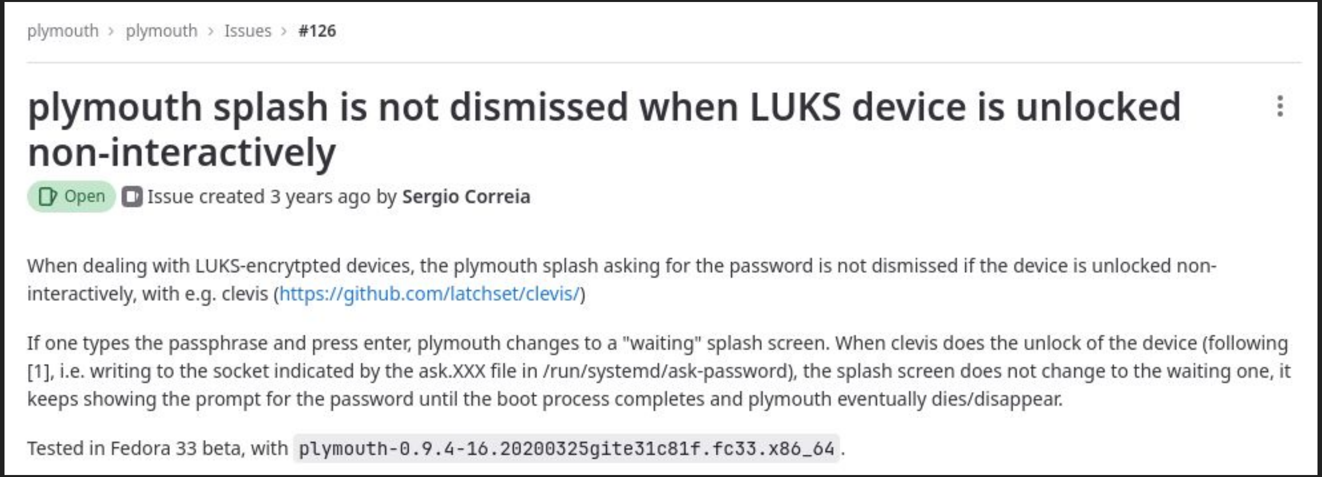


Slow unlock and passphrase request remains during boot #150

Open kowalski7cc opened this issue on Dec 6, 2019 · 12 comments

kowalski7cc commented on Dec 6, 2019

OS: Fedora 31
RPMs: clevis-11-10.fc31.x86_64 manually installed
(The issue is the same as 11-8 from dnf)
After a normal installation `sudo clevis luks bind tpm2 ...` and `sudo dracut -f` unlock happens automatically as expected. But before unlocking happens it take almost 2-3s (On an i7 - NVMe SSD, so it's not performance issue). Also after disk unlock, passphrase request isn't dismissed and remains during boot or upgrade reboot (During updates install remains the passphrase request and under is written the update progress).
One time, I don't know how, I got it to unlock almost istantly and with passphrase request dismissal.



plymouth › plymouth › Issues › **#126**

plymouth splash is not dismissed when LUKS device is unlocked non-interactively

Open Issue created 3 years ago by **Sergio Correia**

When dealing with LUKS-encrytpted devices, the plymouth splash asking for the password is not dismissed if the device is unlocked non-interactively, with e.g. clevis (https://github.com/latchset/clevis/)

If one types the passphrase and press enter, plymouth changes to a "waiting" splash screen. When clevis does the unlock of the device (following [1], i.e. writing to the socket indicated by the ask.XXX file in /run/systemd/ask-password), the splash screen does not change to the waiting one, it keeps showing the prompt for the password until the boot process completes and plymouth eventually dies/disappear.

Tested in Fedora 33 beta, with `plymouth-0.9.4-16.20200325gite31c81f.fc33.x86_64`.

temd
init

systemd-cryptenroll

systemd-measure

systemd v248

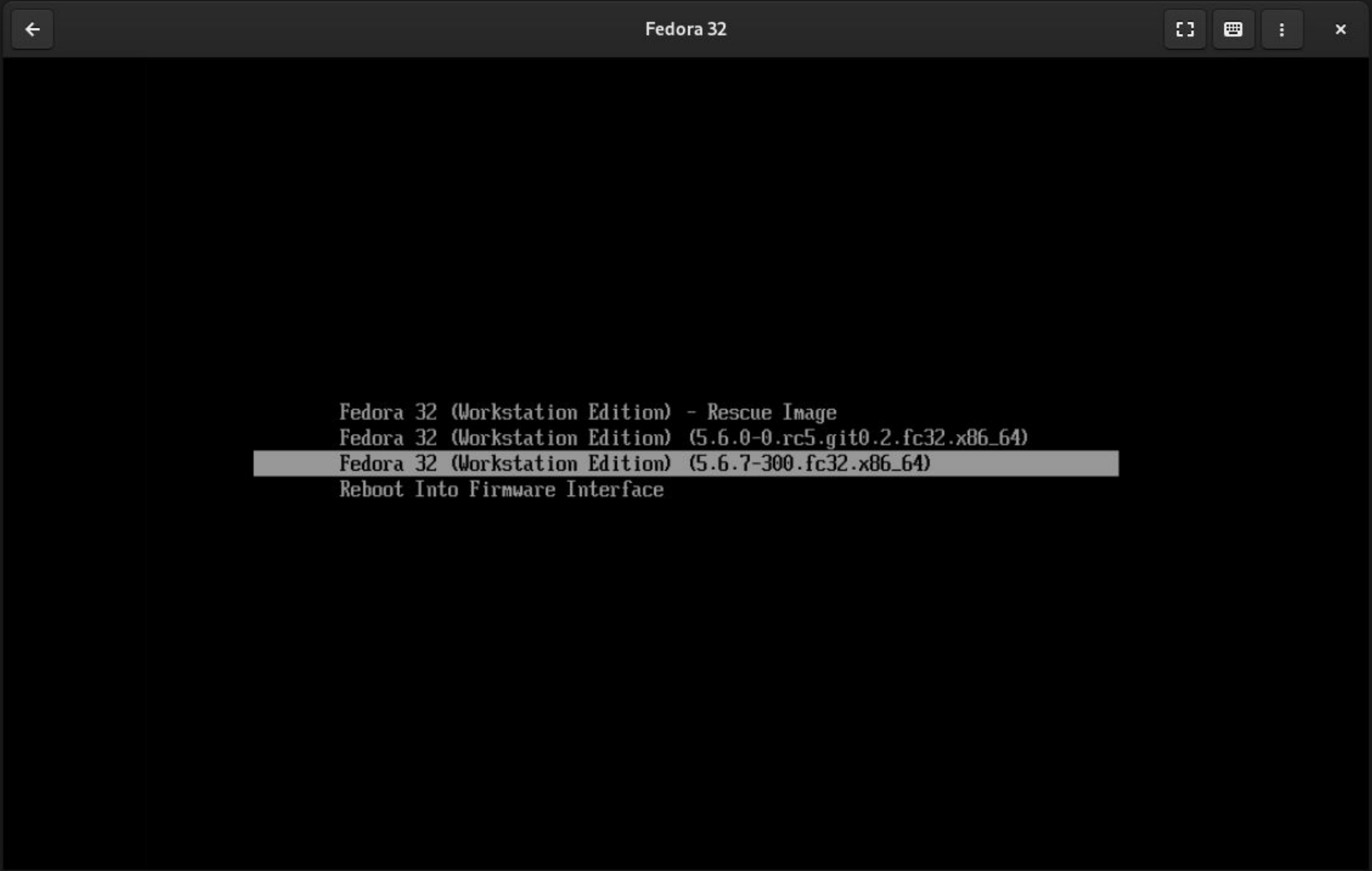
Unlock automatico con systemd-cryptenroll

```
[kowalski7cc@Kaos ~]$ sudo systemd-cryptenroll /dev/nvme0n1p3 --tpm2-device=auto

[kowalski7cc@Kaos ~]$ sudo cryptsetup luksDump /dev/nvme0n1p3
[sudo] password di kowalski7cc:
LUKS header information
Version:        2
...
Tokens:
  0: systemd-tpm2
      tpm2-hash-pcrs:   7
      tpm2-pcr-bank:    sha256
      tpm2-pubkey:
                  (null)
      tpm2-pubkey-pcrs: n/a
      tpm2-primary-alg: ecc
      tpm2-blob: ...
      tpm2-policy-hash: ...
      tpm2-pin:         false
      tpm2-salt:        false
      Keyslot:    1
```

Usare le proprie chiavi?
Usare systemd-bootctl?

systemd-boot: perché?

- Configurazione semplice
- Autodiscovery degli eseguibili EFI
- Veloce (circa 1/3 del tempo di GRUB)
- Minimale



```
Fedora 32 (Workstation Edition) - Rescue Image
Fedora 32 (Workstation Edition) (5.6.0-0.rc5.git0.2.fc32.x86_64)
Fedora 32 (Workstation Edition) (5.6.7-300.fc32.x86_64)
Reboot Into Firmware Interface
```

Cambio di bootloader a systemctl-bootctl

```
[kowalski7cc@Kaos ~]$ # Remove GRUB
[kowalski7cc@Kaos ~]$ sudo bootctl install
[sudo] password di kowalski7cc:

[kowalski7cc@Kaos ~]$ reboot
...

[kowalski7cc@Kaos ~]$ sudo bootctl
[sudo] password di kowalski7cc:
System:
      Firmware: UEFI 2.70 (Lenovo 0.4624)
 Firmware Arch: x64
   Secure Boot: disabled (disabled)
  TPM2 Support: yes
  Boot into FW: supported
```

Cambio di bootloader a systemctl-bootctl

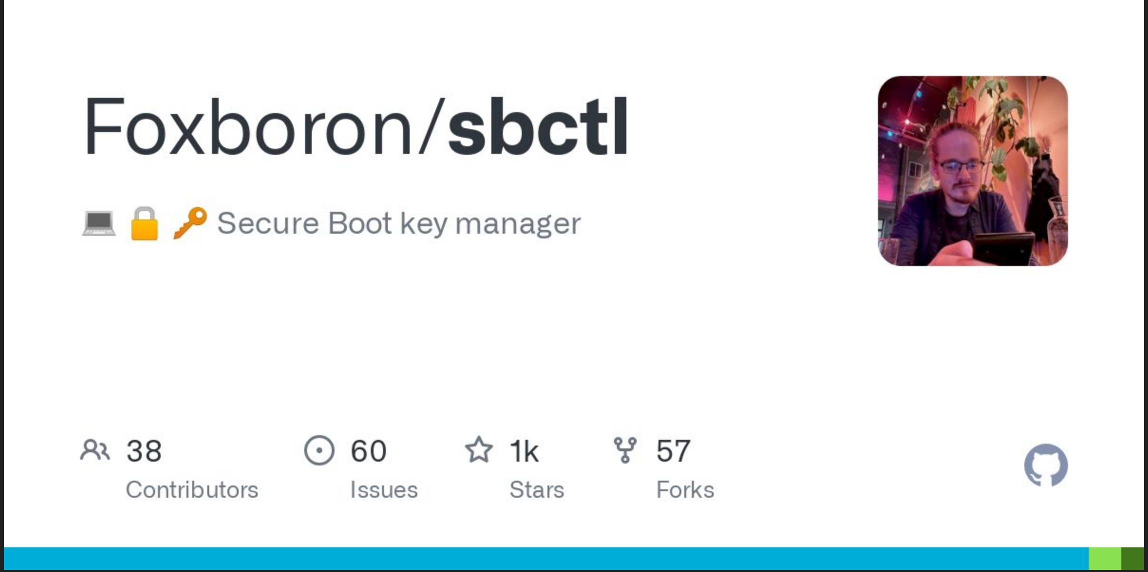
```
Current Boot Loader:
      Product: systemd-boot 253.10-1.fc38
     Features: ✓ Boot counting
               ✓ Menu timeout control
               ✓ One-shot menu timeout control
               ✓ Default entry control
               ✓ One-shot entry control
               ✓ Support for XBOOTLDR partition
               ✓ Support for passing random seed to OS
               ✓ Load drop-in drivers
               ✓ Support Type #1 sort-key field
               ✓ Support @saved pseudo-entry
               ✓ Support Type #1 devicetree field
               ✓ Boot loader sets ESP information
          ESP: /dev/disk/by-partuuid/...
         File: └─/EFI/systemd/systemd-bootx64.efi
```

Cambio di bootloader a systemctl-bootctl

```
Random Seed:
 System Token: set
       Exists: yes

Available Boot Loaders on ESP:
          ESP: /efi (/dev/disk/by-partuuid/...)
         File: ├─/EFI/systemd/systemd-bootx64.efi
               └─/EFI/BOOT/BOOTX64.EFI

Boot Loaders Listed in EFI Variables:
        Title: Linux Boot Manager
           ID: 0x0002
       Status: active, boot-order
    Partition: /dev/disk/by-partuuid/...
         File: └─/EFI/systemd/systemd-bootx64.efi

Boot Loader Entries:
        $BOOT: /efi (/dev/disk/by-partuuid/...)
        token: fedora
```

Cambio di bootloader a systemctl-bootctl

```
Default Boot Loader Entry:
         type: Boot Loader Specification Type #1 (.conf)
        title: Fedora Linux 38 (Workstation Edition) (6.5.6-200.fc38.x86_64)
           id: ...-6.5.6-200.fc38.x86_64.conf
       source: /efi//loader/entries/...-6.5.6-200.fc38.>
     sort-key: fedora
      version: 6.5.6-200.fc38.x86_64
   machine-id: ...
        linux: /efi//.../6.5.6-200.fc38.x86_64/linux
       initrd: /efi//.../6.5.6-200.fc38.x86_64/initrd
      options: root=UUID=... ro rootflags=subvol=@
```



Foxboron/**sbctl**

💻 🔒 🔑 Secure Boot key manager

38 Contributors

60 Issues

1k Stars

57 Forks

https://github.com/Foxboron/sbctl/releases

Firmare gli EFI con la propria chiave

```
[kowalski7cc@Kaos ~]$ sudo sbctl import-keys && sudo sbctl enroll-keys

[kowalski7cc@Kaos ~]$ sudo sbctl verify
Verifying file database and EFI images in /efi...
✓ /efi/a323b96d6ecd4309bc5d0a96bd51939e/0-rescue/linux is signed
‼ /efi/a323b96d6ecd4309bc5d0a96bd51939e/6.3.11-200.fc38.x86_64/linux does not exist
‼ /efi/a323b96d6ecd4309bc5d0a96bd51939e/6.3.7-200.fc38.x86_64/linux does not exist
‼ /efi/a323b96d6ecd4309bc5d0a96bd51939e/6.3.8-200.fc38.x86_64/linux does not exist
✗ /efi/EFI/BOOT/BOOTX64.EFI is not signed
✓ /efi/EFI/systemd/systemd-bootx64.efi is signed
✗ /efi/a323b96d6ecd4309bc5d0a96bd51939e/6.4.15-200.fc38.x86_64/linux is not signed
✗ /efi/a323b96d6ecd4309bc5d0a96bd51939e/6.5.5-200.fc38.x86_64/linux is not signed
✗ /efi/a323b96d6ecd4309bc5d0a96bd51939e/6.5.6-200.fc38.x86_64/linux is not signed

[kowalski7cc@Kaos ~]$ sudo sbctl sign /efi/EFI/BOOT/BOOTX64.EFI
✓ Signed /efi/EFI/BOOT/BOOTX64.EFI
```

Cosa fare se ho driver proprietari con akmod?

Installazione chiave akmod

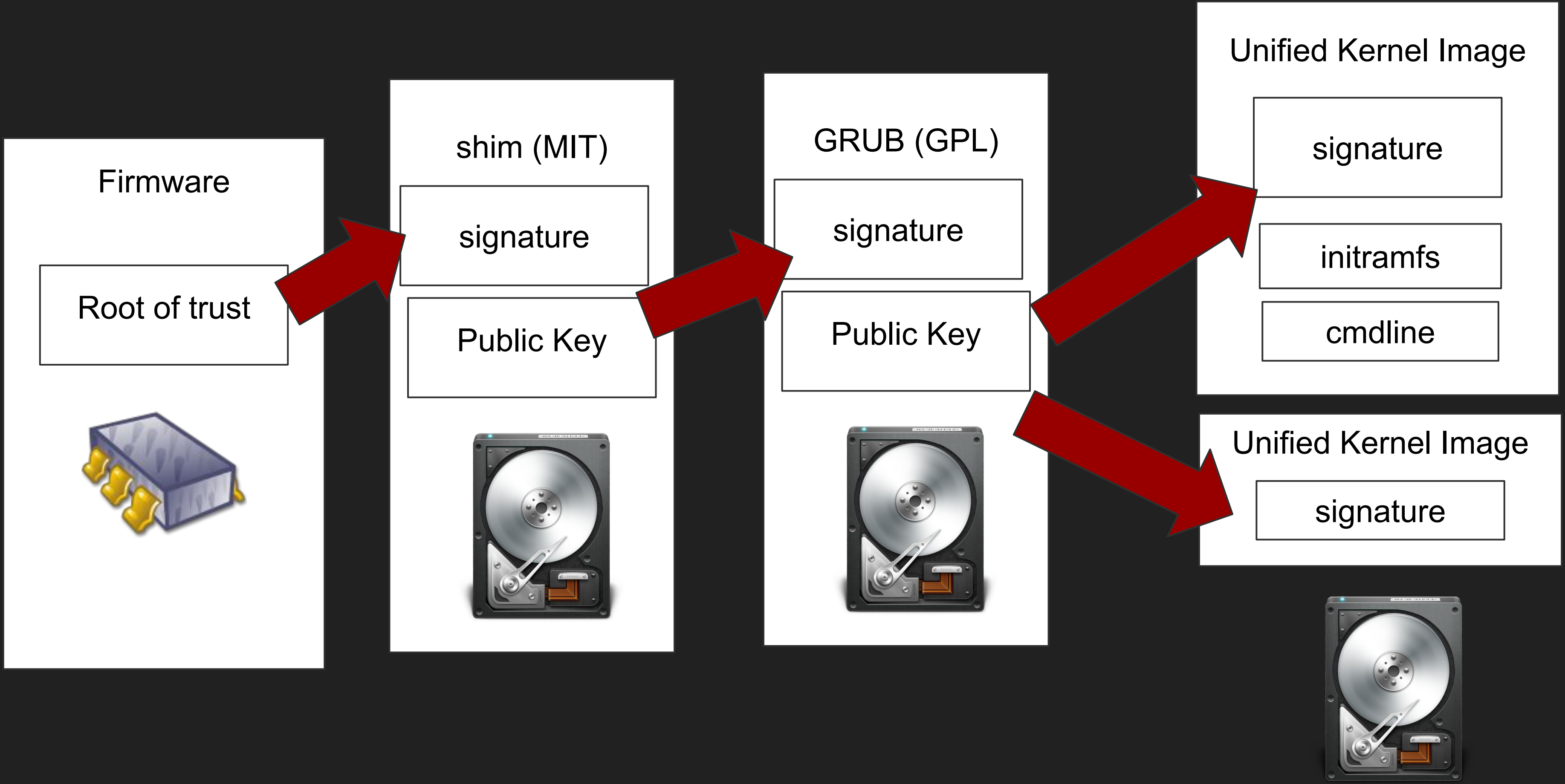
- In ubuntu supportate dal momento dell'installazione con shim/mokutils
- “With Fedora 36+, the akmods package have support to automatically sign locally built kmod with a self generated key. Such key must be imported into the EFI firmware (you must have right to access the EFI firmware).” -rpmfusion

```
[kowalski7cc@Kaos ~]$ sudo mokutil --import /etc/pki/akmods/cers/public_key.der

[kowalski7cc@Kaos ~]$ reboot
...
```

Sviluppi futuri?

Sviluppi futuri

- Automazione del tutto
    - fully signed execution path
    - fully measured execution path
    - easy pre-calculation of expected PCR values
        - easy pre-calculation of expected PCR values
- Full Disk Encryption and Home Encryption as defaults
    - encfs
    - systemd-homed + LUKS
    - BTRFS transparent encryption?
- Unified Kernel Image (UKI)
    - Kernel
    - Initramfs
    - Cmdline
- Signed Kernel Extensions



Firmware

Root of trust

shim (MIT)

signature

Public Key

GRUB (GPL)

signature

Public Key

Unified Kernel Image

signature

initramfs

cmdline

Unified Kernel Image

signature

Thank You!