

Unlock Linux Unified Key Setup (LUKS) encrypted partitions with TPM 2.0


Home (<https://4sysops.com>) / Blog (<https://4sysops.com/archives/>) / Unlock Linux Unified Key Setup (LUKS) encrypted partitions with TPM 2.0

4sysops - The online community for SysAdmins and DevOps

(<https://4sysops.com/archives/update-container-images-with-copa/>)

(<https://4sysops.com/archives/whitelist-a-domain-in-microsoft-365/>)

Tue, Nov 28 2023 (<https://4sysops.com/archives/unlock-linux-unified-key-setup-luks-encrypted-partitions-with-tpm-20/>)

linux, encryption, security 15 

Leveraging TPM 2.0 to unlock Linux Unified Key Setup (LUKS) encrypted partitions ensures an added layer of protection, utilizing hardware-backed security measures to safeguard critical data while automating the unlocking of encrypted drives at boot time.

<

>

Contents

CLOSE

- 01 How TPM2 works
- 02 Enable TPM2 in Linux
- 03 Bind LUKS to TPM2
- 04 Testing, verification, and troubleshooting
- 05 Conclusion



Author Recent Posts

**Evi Vanoost (<https://4sysops.com/members/evanoost/>)**

Evi Vanoost is the Assistant Director for the Office of Research at the University of Rochester. Our teams provide a broad range of IT services, including desktop support, application development, systems administration, server and web hosting, IT consulting, and project management.

(<https://4sysops.com/members/evanoost/>)

Trusted Platform Module 2.0 (TPM2) is a hardware-based security feature designed to provide a secure foundation by storing cryptographic keys and performing various security-related functions. In combination with Secure Boot, it ensures the integrity of the system and helps safeguard sensitive information.

How TPM2 works

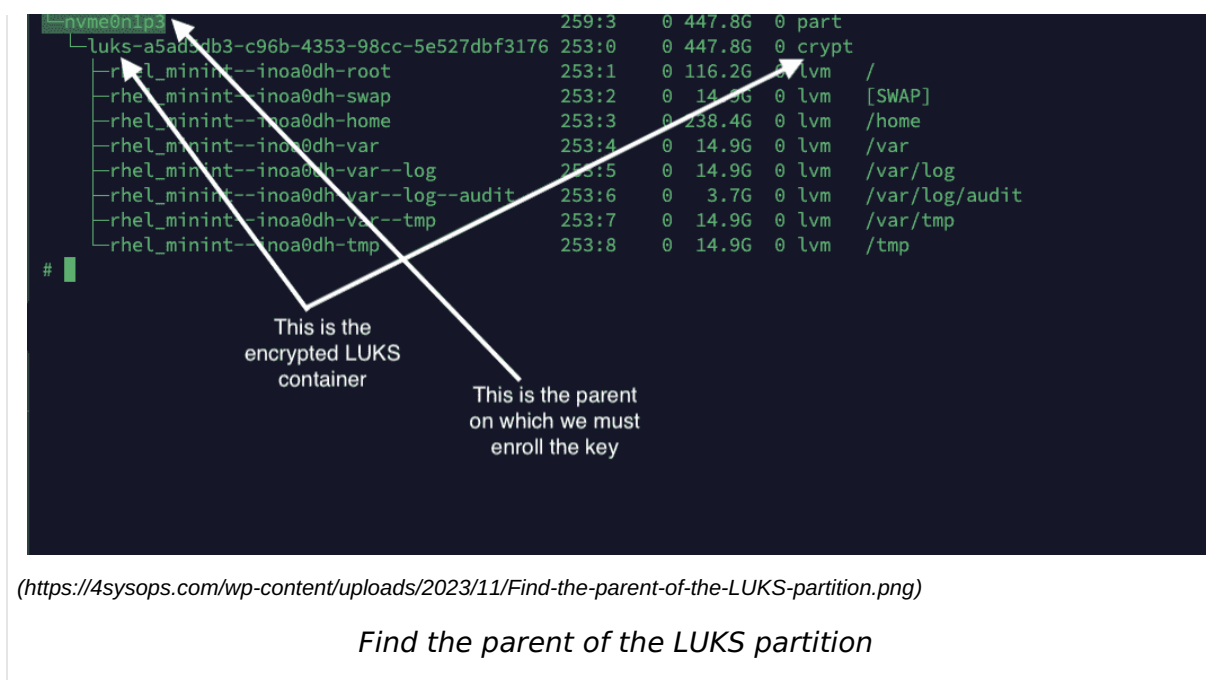
The TPM, in its simplest form, is a storage module that stores cryptographic keys such as private keys for TLS encryption or unlocking an encrypted drive. It also has other functions, such as a hardware random number generator (HW-RNG) and logging features, but we will not focus on those functions in this article.

When a key is requested, the TPM chip measures the hardware, as well as the boot process, and can even be extended to include user-space software. If the hardware has changed or the software and configuration cannot cryptographically verify its integrity, the TPM chip will not return its data.

The TPM chip can store data in various Platform Configuration Registers (PCR). According to the standard (https://trustedcomputinggroup.org/wp-content/uploads/PC-Client-Specific-Platform-TPM-Profile-for-TPM-2p0-v1p05p_r14_pub.pdf), at least 24 registers should be available. Although the exact number may vary based on the chip, within the hardware of your device only the first eight (PCR0 through 7) registers are used. The remaining registers are a

4

```
# lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINTS
nvme0n1                             259:0    0 476.9G  0 disk
├─nvme0n1p1                         259:1    0   200M  0 part  /boot/efi
└─nvme0n1p2                         259:2    0    1G    0 part  /boot
```



available for the boot process but can be extended into specific applications, such as measured boot and remote attestation.

An easy way to remember what each of the first eight registers does is that the even registers (PCR0, 2, 4, and 6) measure physical hardware, and the odd registers measure configuration values in that hardware. PCR0 and 1 measure the UEFI firmware and its settings, PCR2 and 3 measure plugin cards and their settings, and PCR4 and 5 measure the boot loader, disks, and disk partitions. PCR6 is dependent on the platform (on Intel, this is typically reserved to indicate S4 [suspend-to-disk] and S5 [power-off] power events), and PCR7 is the Secure Boot state.

Note that many of the aspects of hardware integrity are also encompassed by Secure Boot, so measuring PCR7 is usually sufficient. On Windows (by default) BitLocker measures PCR7 and 11 (Secure Boot and the integrity of the Windows boot process), or if PCR7 (Secure Boot) is not enabled, it will measure PCR 0, 2, 4 and 11 instead. PCR11 on Linux likewise measures various boot phase values; an overview of what each PCR measures on most modern distros of Linux is available here (https://uapi-group.org/specifications/specs/linux_tpm_pcr_registry/).

The PCRs you should enable before you can unlock a key depend on the level of protection you want and what types of attacks you are protecting against. Enabling too many PCR checks may result in additional service calls, as the TPM locks out the system even if small changes are detected, although in some environments, additional levels of protection may be desirable.



Enable TPM2 in Linux

Before proceeding, verify that your hardware supports TPM2. Many modern systems are equipped with TPM2 modules, either in the CPU or with a dedicated TPM chip on the motherboard. Slightly older systems, equipped with the older TPM1.3, can be upgraded by replacing or adding a TPM2.0 chip from the manufacturer or installing a firmware update.

Make sure to follow any manufacturer instructions on upgrading your firmware or adding components to your motherboard. If you need to add a TPM chip, there is no standard pinout or voltage for TPM chips. Similar-looking modules from different vendors may not be compatible and may result in permanent damage to the system if the correct module is not installed.

Ensure that the TPM2 module is enabled in the system's UEFI settings. Once booted into Linux, your TPM device should show up as 1 or 2 devices in `/dev`. The TPM2 chip's capabilities can be queried using:

1. `tpm2_getcap -l`

```
# ls -l /dev/tpm*
crw-rw---- 1 tss root 10, 224 Oct 8 15:32 /dev/tpm0
crw-rw---- 1 tss tss 253, 65536 Oct 8 15:32 /dev/tpmrm0
# tpm2_getcap -l
- algorithms
- commands
- pcrs
- properties-fixed
- properties-variable
- ecc-curves
- handles-transient
- handles-persistent
- handles-permanent
- handles-pcr
- handles-nv-index
- handles-loaded-session
- handles-saved-session
#
```

(<https://4sysops.com/wp-content/uploads/2023/11/Make-sure-the-TPM-devices-show-up-in-your-Linux-system.png>)

Make sure the TPM devices show up in your Linux system

4

If no TPM device shows up but one is enabled in the UEFI, check with the manufacturer to see whether a driver needs to be loaded.



Create an encrypted LUKS partition (<https://4sysops.com/archives/encrypt-linux-lvm-with-linux-unified-key-setup-luks-using-cockpit/>) and make sure it will attempt to

mount automatically during boot. Many Linux distributions now allow you to create a fully encrypted disk during setup. If you want to have full disk encryption on Linux use that feature to encrypt your disk.

Linux distributions typically provide tools to interface with TPM2 (**systemd cryptenroll**). If none are installed, see my previous articles on creating an encrypted LUKS partition and Secure Boot. On Red Hat distributions (RHEL 9 at the time of writing), the functionality is packed into the Clevis toolset.

Bind LUKS to TPM2

On Ubuntu-based systems, there is a patch we will need to load to make sure that the TPM2 is interrogated during boot. First, we modify **/etc/crypttab**. This file contains the encrypted partitions that should automatically be mounted during boot. We then add a directive to query the first available TPM device:

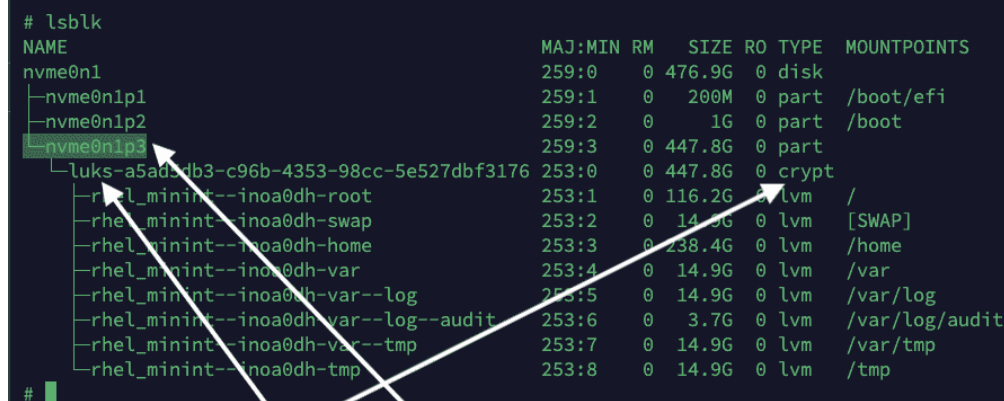
```
1. sed -i 's%%$,tpm2-device=auto%' /etc/crypttab
```

The patch and its documentation can be found here: https://github.com/wmcelderry/systemd_with_tpm2 (https://github.com/wmcelderry/systemd_with_tpm2)

If you want to blindly install it:

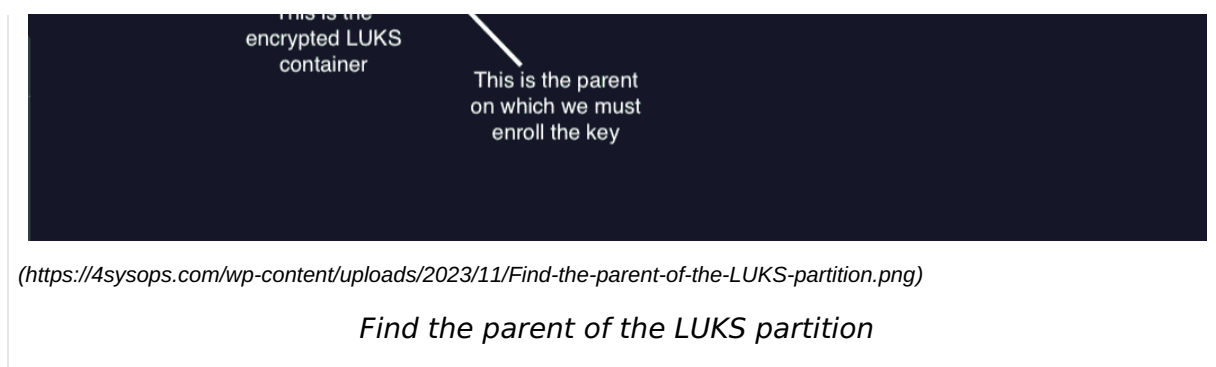
```
1. cd ~
2. apt -y install git
3. git clone https://github.com/wmcelderry/systemd_with_tpm2/
4. cd systemd_with_tpm2
5. sudo ./install.sh
```

On any Linux distribution, **lsblk** will show you which partition contains the encrypted LUKS container for which we want to store the decryption key. This would be the parent of the partition of the type *crypt*.



```
# lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINTS
nvme0n1                             259:0    0 476.9G  0 disk
├─nvme0n1p1                         259:1    0   200M  0 part  /boot/efi
├─nvme0n1p2                         259:2    0    1G    0 part  /boot
└─nvme0n1p3                         259:3    0 447.8G  0 part
   └─luks-a5ad3db3-c96b-4353-98cc-5e527dbf3176 253:0    0 447.8G  0 crypt
      ├─rhel_minint--inoa0dh-root      253:1    0  116.2G  0 lvm    /
      ├─rhel_minint--inoa0dh-swap      253:2    0   14.9G  0 lvm    [SWAP]
      ├─rhel_minint--inoa0dh-home      253:3    0  238.4G  0 lvm    /home
      ├─rhel_minint--inoa0dh-var       253:4    0   14.9G  0 lvm    /var
      ├─rhel_minint--inoa0dh-var--log  253:5    0   14.9G  0 lvm    /var/log
      ├─rhel_minint--inoa0dh-var--log--audit 253:6    0    3.7G  0 lvm    /var/log/audit
      ├─rhel_minint--inoa0dh-var--tmp  253:7    0   14.9G  0 lvm    /var/tmp
      └─rhel_minint--inoa0dh-tmp       253:8    0   14.9G  0 lvm    /tmp
```

This is the



For Ubuntu, we can now use **systemd-cryptenroll** to enroll the encryption key in the TPM device in TPM PCR 7 (Secure Boot); see above for more information or specific PCR registers:

```
1. systemd-cryptenroll --tpm2-device=auto --tpm2-pcrs=7 /dev/nvme0n1p3
```

On Red Hat, we use **clevis** to bind the LUKS encryption to the TPM2 module.

```
1. clevis luks bind -d /dev/nvme0n1p3 tpm2
'{"hash":"sha256","key":"rsa","pcr_bank":"sha256","pcr_ids":"7"}'
```

After entering those commands, you will have to enter a valid unlock password for the partition you have encrypted.

Testing, verification, and troubleshooting

Reboot the system and ensure that the LUKS partition is automatically unlocked using the TPM2 module. Verify that the system boots seamlessly and that the encrypted partition is accessible without manual intervention. If you are having issues verify that your TPM2 module is enabled and that any drivers for it are loaded in the boot image.

Generally, this system will continue to work if Secure Boot can verify the integrity of the boot chain; however, if your hardware changes significantly, you still need to enter a recovery key manually. Like BitLocker on Windows, common reasons for TPM2 failing to unlock are hardware firmware updates or changes in the boot chain (e.g. someone leaves a bootable CD or thumb drive in the system).

Subscribe to 4sysops newsletter!



Subscribe

Conclusion

The fusion of TPM2 technology with encrypted LUKS partitions in Linux is a powerful approach to securing sensitive data. By utilizing hardware-backed security and automating the unlocking process, users can significantly enhance the integrity and confidentiality of their information without sacrificing accessibility.

< 0 Leave a reply



Hi! I am 4sysops AI. Ask a question about this article! Powered by GPT 3.5 Turbo.

(<https://4sysops.com/join/>)Members get free access to an augmented ChatGPT 4 trained with the latest IT content.

Type your question...

Send

IT Administration News

- Microsoft may have broken your VPN with Windows updates (<https://4sysops.com/activity/p/55216/>)
- Windows 11 is losing market share to Windows 10 (<https://4sysops.com/activity/p/55215/>)
- Windows 11 April 2024 Update is causing three major issues (<https://4sysops.com/activity/p/55214/>)
- RAG quickstart with Ray, LangChain, and HuggingFace | Google Cloud Blog (<https://4sysops.com/activity/p/55209/>)
- Amazon EC2 now protects your AMIs from accidental deregistration (<https://4sysops.com/activity/p/55204/>)

Read All IT Administration News (</activity/>)

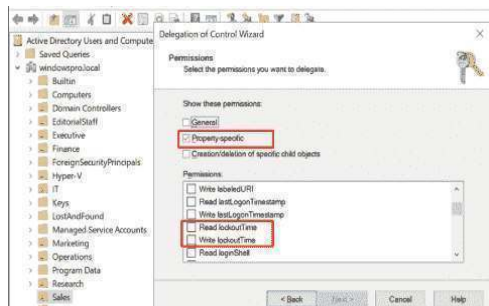


Join our IT community and read articles without ads! (<https://4sysops.com/>)

[join/?utm_source=4sysops&utm_medium=endpage&utm_campaign=NoAds\)](https://4sysops.com/archives/unlock-linux-unified-key-...)

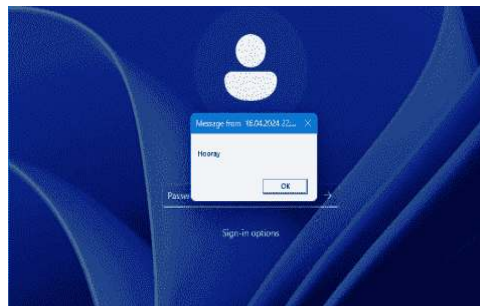
Do you want to write for 4sysops? We are looking for new authors. (https://4sysops.com/write-for-4sysops/?utm_source=4sysops&utm_medium=endpage&utm_campaign=Author)

RELATED ARTICLES



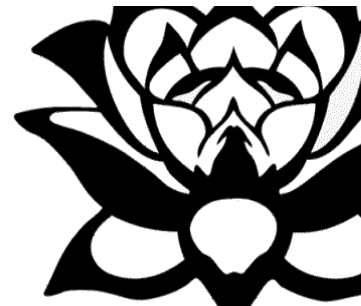
[\(https://4sysops.com/archives/delegate-permission-to-unlock-active-directory-accounts/\)](https://4sysops.com/archives/delegate-permission-to-unlock-active-directory-accounts/)

Delegate permission to unlock Active Directory accounts (<https://4sysops.com/archives/>



[\(https://4sysops.com/archives/allow-end-users-to-execute-code-on-the-windows-logon-screen-with-administrator-privileges/\)](https://4sysops.com/archives/allow-end-users-to-execute-code-on-the-windows-logon-screen-with-administrator-privileges/)

Allow end users to execute code on the Windows logon screen with administrator



[\(https://4sysops.com/archives/new-mitigation:cve-2023-24932-blacklotus-in-the-april-update-not-yet-enabled-by-default/\)](https://4sysops.com/archives/new-mitigation:cve-2023-24932-blacklotus-in-the-april-update-not-yet-enabled-by-default/)

New mitigations for CVE-2023-24932 (BlackLotus) in the Ap

15 COMMENTS



Marcelo Carvalho (<https://www.astranis.com/>)

3 months ago

Hi Evi

Thank you so much for you contribution.

I am puzzled by how difficult has been trying to install LUKS with TPM@.

I have followed a few instructions from different sites and nothing has worked for me on Ubuntu 24.04. I never found specific installation instructions for the 24.04. The HW is Dell Latitude 7440, and confirmed by Dell TPM2 is enabled. Actually the Dell support person laugh at me after I thanked him and said "now I will install TPM2." He adde

“good luck.” That did not go well with me, and now I understand why.

I have done the installation many times and none have worked. I have followed a few different guides.

My last one following your instructions (mainly) I got the boot to freeze and not passing line....

“Set cipher aes, mode xts-platin64, key size 512 for device /dev/nvme-n1p2”

.... and if I try the LUKS passwd it returns....

“Failed to activate with specified passphrase. (passphrase incorrect?)”

Following is my step-by-step implementation.

Step 1) Install U_24.04 with LUKS/LVM

Step 2) Verify if Secure Boot is running.

```
mokutil --sb-state
```

<<<<<<< to me was OK and steps 3/4 skipped.

Step 3) If needed, enable Secure Boot in Linux

```
sudo apt-get install shim-signed grub-efi-amd64-signed
```

```
awk '$2 == "/boot"' /proc/self/mounts
```

```
sudo grub-install /dev/nvme0n1p2 --uefi-secure-boot
```

Step 4) If needed, enroll or restore the Machine Owner Key (MOK)

```
mokutil --import vendor.cer  
mokutil --list-new
```



Step 5) Enable TPM2 in Linux

```
tpm2_getcap -l
```

<<<<<< to view the TPM2 chip's capabilities

Installing tpm2-tools

```
sudo apt update
sudo apt upgrade -y
sudo apt install tpm2-tools
dmesg | grep -i tpm.          <<<<<<<<. To verify
sudo tpm2_getcap -l          <<<<<<<< To validate
```

- algorithms
- commands
- pcrcs
- properties-fixed
- properties-variable
- ecc-curves
- handles-transient
- handles-persistent
- handles-permanent
- handles-pcr
- handles-nv-index
- handles-loaded-session
- handles-saved-session
- vendor

Step 6) Bind LUKS to TPM2:

```
sed -i 's%%$,tpm2-device=auto%' /etc/crypttab
```

My code:

```
sudo diff /etc/crypttab /etc/crypttab.original
```

1c1

```
dm_crypt-0 UUID=632986e7-5d9d-4ffb-a3b2-9cd0c49509b2 none luks
```

4



Step 7) The patch and its documentation can be found here:

https://github.com/wmcelderry/systemd_with_tpm2

If you want to blindly install it: <<<<<<<. Trusted you, blindly.

```
cd ~  
  
apt -y install git  
git clone https://github.com/wmcelderry/systemd_with_tpm2/  
cd systemd_with_tpm2  
sudo ./install.sh
```

Done:

```
# sudo ./install.sh  
# echo $?  
0
```

Step 8) Use systemd-cryptenroll to enroll the encryption key in the TPM device in TPM PCR 7 (Secure Boot)

`systemd-cryptenroll --tpm2-device=auto --tpm2-pcrs=7 /dev/nvme0n1p3`

Executed:

```
sudo systemd-cryptenroll --tpm2-device=auto --tpm2-pcrs=7 /dev/nvme0n1p3
```

 Please enter current passphrase for disk /dev/nvme0n1p3:

New TPM2 token enrolled as key slot 1.

Done - with step #8

Step 9) Testing, verification, and troubleshooting

<https://4sysops.com/archives/unlock-linux-unified-key-setup-luks-encrypt-partitions-with-tpm-20/> <<<<<<<<<< This is here.

"....Reboot the system and ensure that the LUKS partition is automatically unlocked using the TPM2 module...."

Failed



Here we got the boot to freeze and not passing line.... <<<<< As mentione

above.

```
"Set cipher aes, mode xts-platin64, key size 512 for device /dev/nvme-n1p1"
```

.... and if I try the LUKS passwd it returns....

```
"Failed to activate with specified passphrase. (passphrase incorrect?)"
```

Evi, please advise if you see mistakes on my procedures, if you have any steps I am not following, and/or if you have instructions the are specific to Ubuntu 24.04, the release we want to move on using TPM2 with LUKXS.

Many thanks in advance.

Marcelo Carvalho

IT Senior System Administrator

Astranis Space Technologies Corp.

< 0

REPLY ([HTTPS://4SYSOPS.COM/ARCHIVES/UNLOCK-LINUX-UNIFIED-KEY-SETUP-LUKS-ENCRYPTED-PARTITION-WITH-TPM-20/?REPLYTOCOM=1233728#RESPOND](https://4sysops.com/archives/unlock-linux-unified-key-setup-luks-encrypted-partition-with-tpm-20/?replytocom=1233728#RESPOND))



Evi Vanoost (<https://4sysops.com/members/evanoost/>) 3 months ago

Hi,

If you cannot enter the LUKS password manually, then you have another problem that is unrelated to TPM2. The LUKS password should work independently, when you install Ubuntu, there is a way to enable full-disk encryption and there is a checkbox for Secure Boot, both need to be enabled for my instructions to work for Full-Disk Encryption (if that's your goal). If you do that, you shouldn't need to manually update the boot records and kernel etc (the other instructions you post). You can literally enter your FDE password upon boot, apply the systemd patch and use `systemd-cryptenroll`.

One thing I've noticed on some machines is that you have to type the password a bit slower, also if you're on a non-QWERTY keyboard, you may not have your locale loaded at that point (you're in `initrd`).

I haven't tested on Ubuntu 24, but this guide was written for Ubuntu 22.04 LTS and works with the Dell model you describe, we deploy those machines regularly. For Dell, make sure to clear the TPM if you've previously had

Windows installed especially: <https://www.dell.com/support/kbdoc/en-us/000213375/bios-settings-prerequisites-for-ubuntu-22-04-full-disk-encryption-operating-system-installation-or-booting> (<https://www.dell.com/support/kbdoc/en-us/000213375/bios-settings-prerequisites-for-ubuntu-22-04-full-disk-encryption-operating-system-installation-or-booting>)

Also make sure you don't have CSM (BIOS emulation) enabled anywhere in your firmware setting, UEFI-boot only.

E

< 0

[REPLY \(HTTPS://4SYSOPS.COM/ARCHIVES/UNLOCK-LINUX-UNIFIED-KEY-SETUP-LUKS-ENCRYPTED-PARTITION-WITH-TPM-20/?REPLYTOCOM=1233738#RESPOND\)](https://4sysops.com/archives/unlock-linux-unified-key-setup-luks-encrypted-partition-with-tpm-20/?replytocom=1233738#respond)



Marcelo Carvalho (<https://www.astranis.com/>)

3 months ago

I have just posted a comment but do not see here.

Please advise.

Marcelo Carvalho

IT Senior System Administrator

Astranis Space Technologies Corp.

< 0

[REPLY \(HTTPS://4SYSOPS.COM/ARCHIVES/UNLOCK-LINUX-UNIFIED-KEY-SETUP-LUKS-ENCRYPTED-PARTITION-WITH-TPM-20/?REPLYTOCOM=1233729#RESPOND\)](https://4sysops.com/archives/unlock-linux-unified-key-setup-luks-encrypted-partition-with-tpm-20/?replytocom=1233729#respond)



Marcelo Carvalho (<https://www.astranis.com/>)

3 months ago

***** Correcting Step 6. *****

Step 6) Bind LUKS to TPM2:

```
sed -i 's%%$,tpm2-device=auto%' /etc/crypttab
```

My code:



```
sudo diff /etc/crypttab /etc/crypttab.original
1c1
dm_crypt-0 UUID=632986e7-5d9d-4ffb-a3b2-9cd0c49509b2 none luks
```

Many thanks.

_M

< 0

[REPLY \(HTTPS://4SYSOPS.COM/ARCHIVES/UNLOCK-LINUX-UNIFIED-KEY-SETUP-LUKS-ENCRYPTED-PARTITION WITH-TPM-20/?REPLYTOCOM=1233732#RESPOND\)](https://4sysops.com/archives/unlock-linux-unified-key-setup-luks-encrypted-partition-with-tpm-20/?replytocom=1233732#respond)



Marcelo Carvalho (<https://www.astranis.com/>)

3 months ago

ERRATA

Step 6) Bind LUKS to TPM2:

`sed -i 's%%$,tpm2-device=auto%' /etc/crypttab`

My code:

```
sudo diff /etc/crypttab /etc/crypttab.original
1c1
dm_crypt-0 UUID=632986e7-5d9d-4ffb-a3b2-9cd0c49509b2 none luks
```

< 0

[REPLY \(HTTPS://4SYSOPS.COM/ARCHIVES/UNLOCK-LINUX-UNIFIED-KEY-SETUP-LUKS-ENCRYPTED-PARTITION WITH-TPM-20/?REPLYTOCOM=1233733#RESPOND\)](https://4sysops.com/archives/unlock-linux-unified-key-setup-luks-encrypted-partition-with-tpm-20/?replytocom=1233733#respond)



Marcelo Carvalho (<https://www.astranis.com/>)

3 months ago

O Step 6, the following line is not showing on previous postings



```
dm_crypt-0 UUID=632986e7-5d9d-4fffb-a3b2-9cd0c49509b2 none luks,tpm2-device=auto
```

This is the final value of file /etc/crypttab.

Many thanks'

_M < 0

[REPLY \(HTTPS://4SYSOPS.COM/ARCHIVES/UNLOCK-LINUX-UNIFIED-KEY-SETUP-LUKS-ENCRYPTED-PARTITION WITH-TPM-20/?REPLYTOCOM=1233735#RESPOND\)](https://4sysops.com/archives/unlock-linux-unified-key-setup-luks-encrypted-partition-with-tpm-20/?replytocom=1233735#RESPOND)



Evi Vanoost (<https://4sysops.com/members/evanoost/>) 3 months ago

dm_crypt0?

It should be nvme0n1p3_crypt UUID=...

How did you encrypt (manual partition?), RAID? Are you doing FDE during install? May be an artifact of Ubuntu 24 which I haven't tested yet.

Do lsblk – mine looks like this:

```
└─nvme0n1p3 259:3 0 463.6G 0 part
└─nvme0n1p3_crypt 253:0 0 463.6G 0 crypt
└─vgubuntu-root 253:1 0 128G 0 lvm
```

< 0

[REPLY \(HTTPS://4SYSOPS.COM/ARCHIVES/UNLOCK-LINUX-UNIFIED-KEY-SETUP-LUKS-ENCRYPTED-PARTITION WITH-TPM-20/?REPLYTOCOM=1233742#RESPOND\)](https://4sysops.com/archives/unlock-linux-unified-key-setup-luks-encrypted-partition-with-tpm-20/?replytocom=1233742#RESPOND)



Marcelo Carvalho (<https://www.astranis.com/>)

3 months ago

Hi EVi

Thanks for the quick turn around.

I will have to rinse-n-repeat, since it is not booting.

I will follow up with you as soon I get it back.

Many thank



_M

< 0

REPLY (<https://4sysops.com/archives/unlock-linux-unified-key-setup-luks-encrypted-partition-with-tpm-20/?replytocom=1233745#respond>)



Marcelo Carvalho (<https://www.astranis.com/>)

3 months ago

Hi Evi

I have repeat steps 1 through 5 and now, before moving on with step 6, your scrip, this is my state.

```
cat /etc/crypttab
dm_crypt-0 UUID=b02ca9e7-37c8-42d2-82f8-ceaec1fe1d6d none luks

Latitude-7440:~$ lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINTS
.....
nvme0n1                             259:0    0 953.9G  0 disk
├─nvme0n1p1                         259:1    0     1G  0 part  /boot/efi
├─nvme0n1p2                         259:2    0     2G  0 part  /boot
└─nvme0n1p3                         259:3    0 950.8G  0 part
    └─dm_crypt-0                    252:0    0 950.8G  0 crypt
        └─ubuntu--vg-ubuntu--lv
            252:1    0 950.8G  0 lvm    /var/snap/firefox/common/host-
hunspell
                                     /snap
```

It seams the original /etc/crypttab caries dm_crypt-0 as output of lsblk shows.

Looks reasonable the sed command did not change.

I think I am good here.

I will go forward and post my results later.

My concern is at Step 8.

If this line is correct in my case:

4



```
sudo systemd-cryptenroll --tpm2-device=auto --tpm2-pcrs=7 /dev/nvme0n1p3
```

Is this line OK for me on the /dev/nvme0n1p3?

Please advise.

Many thanks,

_M

< 0

REPLY ([HTTPS://4SYSOPS.COM/ARCHIVES/UNLOCK-LINUX-UNIFIED-KEY-SETUP-LUKS-ENCRYPTED-PARTITION-WITH-TPM-20/?REPLYTOCOM=1233889#RESPOND](https://4sysops.com/archives/unlock-linux-unified-key-setup-luks-encrypted-partition-with-tpm-20/?replytocom=1233889#respond))



Evi Vanoost (<https://4sysops.com/members/evanoost/>) 3 months ago

If the patches hold, it should work.

< 0

REPLY ([HTTPS://4SYSOPS.COM/ARCHIVES/UNLOCK-LINUX-UNIFIED-KEY-SETUP-LUKS-ENCRYPTED-PARTITION-WITH-TPM-20/?REPLYTOCOM=1233891#RESPOND](https://4sysops.com/archives/unlock-linux-unified-key-setup-luks-encrypted-partition-with-tpm-20/?replytocom=1233891#respond))

<



Marcelo Carvalho (<https://www.astranis.com/>)

3 months ago

>

Hi Evi.

Done with installation and configuration.

Do you have any recommendation to test actual configuration before reboot?

Please advise. In process of rebooting following.

Many thanks

_M

< 0

REPLY ([HTTPS://4SYSOPS.COM/ARCHIVES/UNLOCK-LINUX-UNIFIED-KEY-SETUP-LUKS-ENCRYPTED-PARTITION-WITH-TPM-20/?REPLYTOCOM=1234125#RESPOND](https://4sysops.com/archives/unlock-linux-unified-key-setup-luks-encrypted-partition-with-tpm-20/?replytocom=1234125#respond))



4





Marcelo Carvalho (<https://www.astranis.com/>)

3 months ago

Hi Evi

I am sorry to say but it did not work.

I just rebooted the system and it stopped at LUKS password prompt. It passed the prompt with the password typed in and all is working on the system, but not the TPM2 LUKS bypass as expected.

Here is dmesg output:

```
Latitude-7440:~$ sudo dmesg | grep -i tpm
[sudo] password for astranis-admin:
[      0.000000] efi: ACPI=0x617fe000 ACPI 2.0=0x617fe014 SMBIOS=0x4d498000 TPM
FinalLog=0x614cb000 ESRT=0x4d430718 MEMATTR=0x473ef018 MOKvar=0x4d464000 INITRD=
0x4742bf98 RNG=0x61716018 TPMEventLog=0x472cb018
[      0.005110] ACPI: SSDT 0x00000000617FD000 00060E (v02 DELL   Tpm2Tab1 0000
1000 INTL 20200717)
[      0.005111] ACPI: TPM2 0x0000000061726000 00004C (v04 DELL   Dell Inc 0000
0002   01000013)
[      0.005137] ACPI: Reserving TPM2 table memory at [mem 0x61726000-0x6172604
b]
[      1.131962] tpm_tis STM0176:00: 2.0 TPM (device-id 0x0, rev-id 78)
[   68.941631] systemd[1]: systemd 253.5-1ubuntu7 running in system mode (+PAM
+AUDIT +SELINUX +APPARMOR +IMA +SMACK +SECCOMP +GCRYPT -GNUTLS +OPENSSL +ACL +BL
KID +CURL +ELFUTILS +FIDO2 +IDN2 -IDN +IPTC +KMOD +LIBCRYPTSETUP +LIBFDISK +PCRE
2 -PWQUALITY +P11KIT +QRENCODE +TPM2 +BZIP2 +LZ4 +XZ +ZLIB +ZSTD -BPF_FRAMEWORK
-XKBCOMMON +UTMP +SYSVINIT default-hierarchy=unified)
[   69.124409] systemd[1]: systemd-pcrmachine.service - TPM2 PCR Machine ID Meas
urement was skipped because of an unmet condition check (ConditionPathExists=/sy
s/firmware/efi/efivars/StubPcrKernelImage-4a67b082-0a4c-41cf-b6c7-440b29bb8c4f).
```

Does it tells us anything.

```
.....systemd-pcrmachine.service - TPM2 PCR Machine ID Measurement was skipped b
ecause of an unmet condition check (ConditionPathExists=/sys/firmware/efi/efivar
s/StubPcrKernelImage-4a67b082-0a4c-41cf-b6c7-440b29bb8c4f).....
```



I am sorry for the spam but here is journalctl -b output for tpm



```
astranis-admin@Latitude-7440:~$ sudo journalctl -b | grep -i tpm
Jan 29 08:53:46 Latitude-7440 kernel: efi: ACPI=0x617fe000 ACPI 2.0=0x617fe014 S
MBIOS=0x4d498000 TPMFinalLog=0x614cb000 ESRT=0x4d430718 MEMATTR=0x473ef018 MOKVa
r=0x4d464000 INITRD=0x4742bf98 RNG=0x61716018 TPMEventLog=0x472cb018
Jan 29 08:53:46 Latitude-7440 kernel: ACPI: SSDT 0x00000000617FD000 00060E (v02
DELL Tpm2Tabl 00001000 INTL 20200717)
Jan 29 08:53:46 Latitude-7440 kernel: ACPI: TPM2 0x0000000061726000 00004C (v04
DELL Dell Inc 00000002 01000013)
Jan 29 08:53:46 Latitude-7440 kernel: ACPI: Reserving TPM2 table memory at [mem
0x61726000-0x6172604b]
Jan 29 08:53:46 Latitude-7440 kernel: tpm_tis STM0176:00: 2.0 TPM (device-id 0x0
, rev-id 78)
Jan 29 08:53:46 Latitude-7440 systemd[1]: systemd 253.5-1ubuntu7 running in syst
em mode (+PAM +AUDIT +SELINUX +APPARMOR +IMA +SMACK +SECCOMP +GCRYPT -GNUTLS +OP
ENSSL +ACL +BLKID +CURL +ELFUTILS +FIDO2 +IDN2 -IDN +IPTC +KMOD +LIBCRYPTSETUP
+LIBFDISK +PCRE2 -PWQUALITY +P11KIT +QRENCODE +TPM2 +BZIP2 +LZ4 +XZ +ZLIB +ZSTD
-BPF_FRAMEWORK -XKBCOMMON +UTMP +SYSVINIT default-hierarchy=unified)
Jan 29 08:53:46 Latitude-7440 systemd[1]: systemd-pcrmachine.service - TPM2 PCR
Machine ID Measurement was skipped because of an unmet condition check (Conditio
nPathExists=/sys/firmware/efi/efivars/StubPcrKernelImage-4a67b082-0a4c-41cf-b6c
7-440b29bb8c4f).
Jan 29 08:53:46 Latitude-7440 systemd[1]: systemd-pcrmachine.service - TPM2 PCR
Machine ID Measurement was skipped because of an unmet condition check (Conditio
nPathExists=/sys/firmware/efi/efivars/StubPcrKernelImage-4a67b082-0a4c-41cf-b6c
7-440b29bb8c4f).
Jan 29 08:53:46 Latitude-7440 systemd[1]: systemd-pcrmachine.service - TPM2 PCR
Machine ID Measurement was skipped because of an unmet condition check (Conditio
nPathExists=/sys/firmware/efi/efivars/StubPcrKernelImage-4a67b082-0a4c-41cf-b6c
7-440b29bb8c4f).
Jan 29 08:53:46 Latitude-7440 systemd[1]: systemd-pcrmachine.service - TPM2 PCR
Machine ID Measurement was skipped because of an unmet condition check (Conditio
nPathExists=/sys/firmware/efi/efivars/StubPcrKernelImage-4a67b082-0a4c-41cf-b6c
7-440b29bb8c4f).
Jan 29 08:53:47 Latitude-7440 systemd[1]: systemd-pcrmachine.service - TPM2 PCR
Machine ID Measurement was skipped because of an unmet condition check (Conditio
nPathExists=/sys/firmware/efi/efivars/StubPcrKernelImage-4a67b082-0a4c-41cf-b6c
7-440b29bb8c4f).
Jan 29 08:53:49 Latitude-7440 systemd[1]: tpm-udev.path - Handle dynamically add
ed tpm devices was skipped because of an unmet condition check (ConditionVirtual
ization=container).
```



```
Jan 29 08:53:49 Latitude-7440 systemd[1]: systemd-pcrphase-sysinit.service - TPM
2 PCR Barrier (Initialization) was skipped because of an unmet condition check
(ConditionPathExists=/sys/firmware/efi/efivars/StubPcrKernelImage-4a67b082-0a4
c-41cf-b6c7-440b29bb8c4f).
Jan 29 08:53:49 Latitude-7440 systemd[1]: systemd-pcrphase.service - TPM2 PCR Ba
rrier (User) was skipped because of an unmet condition check (ConditionPathExist
s=/sys/firmware/efi/efivars/StubPcrKernelImage-4a67b082-0a4c-41cf-b6c7-440b29bb8
c4f).
```

It also shows

```
"systemd-pcrphase.service - TPM2 PCR Barrier (User) was skipped because of an un
met condition check (ConditionPathExists=/sys/firmware/efi/efivars/StubPcrKernel
Image-4a67b082-0a4c-41cf-b6c7-440b29bb8c4f)."
```

Please, any advice?

Many thanks.

_M

<

< 0

>


REPLY (<https://4sysops.com/archives/unlock-linux-unified-key-setup-luks-encrypted-partition-with-tpm-20/?replytocom=1234859#RESPOND>)



Evi Vanoost (<https://4sysops.com/members/evanoost/>) 3 months ago

The error says what the issue is, namely that your TPM could not find or measure the validity of the pre-boot Kernel image.

Potential fixes

- Clear and Activate TPM 2.0 in the UEFI (then start again from the systemd-cryptenroll point)
- Activate Secure Boot in the Secure Boot section of the UEFI configurati
- You are enabling third party drivers (eg. nVIDIA) during setup (the kerne stub is not signed or not signed with something your UEFI BIOS will accept).
- You are using a Linux kernel binary that has not been signed (ye )

Given you are running a pre-release Ubuntu distro, I would file a bug repor

with Ubuntu as it is likely a bug or they have not signed the proper binaries. It is also possible that they do not sign pre-release systems and may have different key for development environments which you have to manually load.

 < +2



(<https://4sysops.com/members/michael-pietroforte/>)

REPLY (<https://4sysops.com/archives/unlock-linux-unified-key-setup-luks-encrypted-partition-with-tpm-20/?replytocom=1234863#respond>)



Marcelo Carvalho (<https://www.astranis.com/>)

3 months ago

Some more output worth mentioning.




```
Latitude-7440:~$ sudo snap recovery --show-keys
```

```
error: system does not use disk encryption
```

```
Latitude-7440:~$ sudo apt list --upgradable
```

```
Listing... Done
```

```
Latitude-7440:~$ lsblk
```

NAME	MAJ:MIN	RM	SIZE	RO	TYPE	MOUNTPOINTS
loop0	7:0	0	4K	1	loop	/snap/bare/5 /snap/bare/5
loop1	7:1	0	74.1M	1	loop	/snap/core22/1033 /snap/core22/1033
loop2	7:2	0	246M	1	loop	/snap/firefox/3626 /snap/firefox/3626
loop3	7:3	0	11.2M	1	loop	/snap/firmware-update r/109 /snap/firmware-updater/1 09
loop4	7:4	0	497M	1	loop	/snap/gnome-42-2204/14 1 /snap/gnome-42-2204/141
loop5	7:5	0	91.7M	1	loop	/snap/gtk-common-theme s/1535 /snap/gtk-common-themes/ 1535
loop6	7:6	0	10.5M	1	loop	/snap/snap-store/1046 /snap/snap-store/1046
loop7	7:7	0	40.4M	1	loop	/snap/snapd/20671 /snap/snapd/20671
loop8	7:8	0	452K	1	loop	/snap/snapd-desktop-in tegration/83 /snap/snapd-desktop-inte gration/83
nvme0n1	259:0	0	953.9G	0	disk	
└─nvme0n1p1	259:1	0	1G	0	part	/boot/efi
└─nvme0n1p2	259:2	0	2G	0	part	/boot
└─nvme0n1p3	259:3	0	950.8G	0	part	
└─dm_crypt-0	252:0	0	950.8G	0	crypt	
└─ubuntu--vg-ubuntu--lv	252:1	0	950.8G	0	lvm	/var/snap/firefox/comm



```
on/host-hunspell
```

```
/snap
```

```
/
```

Thanks

_M

< 0

REPLY ([HTTPS://4SYSOPS.COM/ARCHIVES/UNLOCK-LINUX-UNIFIED-KEY-SETUP-LUKS-ENCRYPTED-PARTITION-WITH-TPM-20/?REPLYTOCOM=1234861#RESPOND](https://4sysops.com/archives/unlock-linux-unified-key-setup-luks-encrypted-partition-with-tpm-20/?replytocom=1234861#respond))



Marcelo Carvalho (<https://www.astranis.com/>)

3 months ago

Thank you so much Evi.

At this point we are putting the breaks on it.

We will wait for more stable release of 24.04 to try again.

I appreciate your help and will keep in touch.

Many thanks.

Marcelo Carvalho

IT Senior System Administrator

< 0

REPLY ([HTTPS://4SYSOPS.COM/ARCHIVES/UNLOCK-LINUX-UNIFIED-KEY-SETUP-LUKS-ENCRYPTED-PARTITION-WITH-TPM-20/?REPLYTOCOM=1234908#RESPOND](https://4sysops.com/archives/unlock-linux-unified-key-setup-luks-encrypted-partition-with-tpm-20/?replytocom=1234908#respond))

Leave a reply

Please enclose code in pre tags: `<pre></pre>`

Your email address will not be published. Required fields are marked *

4

Comment



Name *

Email*

Website

<

☒ Notify me of followup comments via e-mail. You can also subscribe (<https://4sysops.com/comments/subscriptions/?srp=1577641&srk=&sra=s&srsrc=f>) without commenting.

>

POST COMMENT

☐ Receive new post notifications

Subscribe to Newsletter



Subscribe

Follow 4sysops



(<https://twitter.com/4sysops/>)



(<https://www.facebook.com/4sysops>)



(<https://www.linkedin.com/company/4sysops/>)



(<https://4sysops.com/feed/>)

© 4sysops 2006 - 2024

WindowsUpdatePreventer (<https://4sysops.com/windowsupdatepreventer-for-windows>)

