

# LUKS + TPM2 + auto unlock at boot (systemd-cryptenroll)

Asked 1 year ago   Modified 2 months ago   Viewed 7k times

---



4



Please, help me to finish setup LUKS + TPM2 + auto unlock at boot.

I have installed clean Ubuntu 22.04.2 I have encrypted partition in GUI while installing OS.  
I have installed all updates.

Ubuntu 22.04.2 LTS  
5.19.0-43-generic  
systemd 249 (249.11-0ubuntu3.9)

I am trying to use this manual: [https://wiki.archlinux.org/title/Trusted\\_Platform\\_Module#systemd-cryptenroll](https://wiki.archlinux.org/title/Trusted_Platform_Module#systemd-cryptenroll)

I have installed:

```
tpm2-tools  
dracut-core_059-3_amd64.deb  
dracut_059-3_all.deb
```

Next:

```
sudo dracut --add tpm2-tss  
sudo systemd-cryptenroll --tpm2-device=auto --tpm2-pcrs=0+7 /dev/nvme0n1p3
```

I have added in `/etc/crypttab` :

```
nvme0n1p3_crypt UUID=1fce6364-485c-4524-9c73-7bd4dac5bd32 none luks,discard
```

System still asking for a passphrase while booting.

I am do not understand what I need to do exactly to auto-unlock LUKS via TPM on boot.

luks

tpm

Share Follow

asked Jun 2, 2023 at 12:00



Vasiliy

41 1 4

2 Answers

Sorted by: Highest score (default)





6

This is what I'm using to allow LUKS decryption using TPM2 in the same Ubuntu 22. Not using systemd-cryptenroll, but clevis. The only 'downside' is that it shows the password prompt at boot, but disappears after getting the key from tpm.



```
#!/bin/bash

#install needed packages
apt-get -y install clevis clevis-tpm2 clevis-luks clevis-initramfs
initramfs-tools tss2

#proceed
echo -n Enter LUKS password:
read -s LUKSKEY
echo ""

clevis luks bind -d /dev/nvme0n1p3 tpm2 '{"pcr_bank":"sha256"}' <<<
"$LUKSKEY"

update-initramfs -u -k all

#check
clevis luks list -d /dev/nvme0n1p3

#delete example; -s is one of the slots reported by the previous command
#clevis luks unbind -d /dev/nvme0n1p3 -s 1 tpm2
```

No need to modify anything else(not even crypttab file).

Share Follow

edited Jun 28, 2023 at 11:16

answered Jun 28, 2023 at 11:15



Ionel P

61 3

Thank you! I will try it. I have tried to use "build-in" (systems) to unlock LUKS. – Vasiliy Jun 29, 2023 at 11:34

Thank God for you! This information was so convoluted to find, and this was so succinct and easy, and worked! – blisstdev Aug 29, 2023 at 4:36

I was worried about the device name /dev/nvme0n1p3 being hard coded but on my fresh install I had the exact same disk so it worked without modification. – Chris Magnuson Mar 14 at 2:16



I see just one issue in your steps in the `/etc/crypttab` . It is required to add `tpm2-device=auto` .

1

Here is the updated file



```
nvme0n1p3_crypt UUID=1fce6364-485c-4524-9c73-7bd4dac5bd32 none tpm2-  
device=auto,luks,discard
```



Once `/etc/crypttab` updated run `dracut -f`

If these details won't be enough there is [detailed guide](#) with only one major difference comparing to your step. I am not fully sure if `dracut_059` compatible with Ubuntu 22.04 since Ubuntu is shipped with 051 release. As a workaround I just added few dracut modules folders into 051 release manually.

```
01systemd-sysusers  
01systemd-udev  
91tpm2-tss
```

Share Follow

answered Apr 14 at 10:12



Kiryl

11 1