

Advanced Encryption Options Land in the YaST Partitioner

By *Roy Schestowitz*

Created *09/10/2019 - 3:20pm*

Submitted by Roy Schestowitz on Wednesday 9th of October 2019 03:20:53 PM Filed under [GNU](#) [1] [Linux](#) [2] [SUSE](#) [3]

As you may know, so far the YaST Partitioner offered an "Encrypt Device" checkbox when creating or editing a block device. If such box is marked, the Partitioner asks for an encryption password and creates a LUKS virtual device on top of the device being encrypted.

LUKS (Linux Unified Key Setup) is the standard for Linux hard disk encryption. By providing a standard on-disk-format, it facilitates compatibility among distributions. LUKS stores all necessary setup information in the partition header, enabling to transport or migrate data seamlessly. So far, there are two format specifications for such header: LUKS1 and LUKS2. YaST uses LUKS1 because is established, solid and well-known, being fully compatible with the (open)SUSE installation process and perfectly supported by all the system tools and by most bootloaders, like Grub2.

You should not fix what is not broken. Thus, in most cases, the screen for encrypting a device has not changed at all and it still works exactly in the same way under the hood.

[4]

[GNU Linux SUSE](#)

Source URL: <http://www.tuxmachines.org/node/129081>

Links:

[1] <http://www.tuxmachines.org/taxonomy/term/144>

[2] <http://www.tuxmachines.org/taxonomy/term/63>

[3] <http://www.tuxmachines.org/taxonomy/term/117>

[4] <https://lizards.opensuse.org/2019/10/09/advanced-encryption-yast/>