



Full credit is given to the above companies including the Operating System (OS) that this PDF file was generated!

Rocky Enterprise Linux 9.2 Manual Pages on command 'systemd-cryptsetup.8'

\$ man systemd-cryptsetup.8

SYSTEMD-CRYPTSETUP@.SERVICE(8) systemd-cryptsetup@.service SYSTEMD-CRYPTSETUP@.SERVICE(8)

NAME

systemd-cryptsetup@.service, systemd-cryptsetup - Full disk decryption logic

SYNOPSIS

systemd-cryptsetup@.service

system-systemd\x2dcryptsetup.slice

/lib/systemd/systemd-cryptsetup

DESCRIPTION

systemd-cryptsetup@.service is a service responsible for setting up encrypted block devices. It is instantiated for each device that requires decryption for access.

systemd-cryptsetup@.service instances are part of the system-systemd\x2dcryptsetup.slice slice, which is destroyed only very late in the shutdown procedure. This allows the encrypted devices to remain up until filesystems have been unmounted.

systemd-cryptsetup@.service will ask for hard disk passwords via the password agent logic[1], in order to query the user for the password using the right mechanism at boot and during runtime.

At early boot and when the system manager configuration is reloaded, /etc/crypttab is translated into systemd-cryptsetup@.service units by systemd-cryptsetup-generator(8).

In order to unlock a volume a password or binary key is required.

systemd-cryptsetup@.service tries to acquire a suitable password or binary key via the following mechanisms, tried in order:

1. If a key file is explicitly configured (via the third column in /etc/crypttab), a key

read from it is used. If a PKCS#11 token, FIDO2 token or TPM2 device is configured

(using the `pkcs11-uri=`, `fido2-device=`, `tpm2-device=` options) the key is decrypted before use.

2. If no key file is configured explicitly this way, a key file is automatically loaded from `/etc/cryptsetup-keys.d/volume.key` and `/run/cryptsetup-keys.d/volume.key`, if present. Here too, if a PKCS#11/FIDO2/TPM2 token/device is configured, any key found this way is decrypted before use.
3. If the `try-empty-password` option is specified it is then attempted to unlock the volume with an empty password.
4. The kernel keyring is then checked for a suitable cached password from previous attempts.
5. Finally, the user is queried for a password, possibly multiple times, unless the `headless` option is set.

If no suitable key may be acquired via any of the mechanisms describes above, volume activation fails.

SEE ALSO

`systemd(1)`, `systemd-cryptsetup-generator(8)`, `crypttab(5)`, `systemd-cryptenroll(1)`, `cryptsetup(8)`

NOTES

1. password agent logic

https://systemd.io/PASSWORD_AGENTS/

systemd 249

SYSTEMD-CRYPTSETUP@.SERVICE(8)