NAME

cryptsetup-tcryptDump − dump the header information of a TCRYPT (TrueCrypt or VeraCrypt compatible) device

SYNOPSIS

cryptsetup *tcryptDump* **[<options>] <device>**

DESCRIPTION

Dump the header information of a TCRYPT (TrueCrypt or VeraCrypt compatible) device.

If the −−dump−volume−key option is used, the TCRYPT device volume key is dumped instead of the TCRYPT header info. Beware that the volume key (or concatenated volume keys if a cipher chain is used) can be used to decrypt the data stored in the TCRYPT container without a passphrase. This means that if the volume key is compromised, the whole device has to be erased to prevent further access. Use this option carefully.

The −−key−file option allows a combination of file content with the passphrase The −−key−file option can be repeated. Note that using keyfiles differs from LUKS keyfile logic.

<options> can be [−−dump−volume−key, −−key−file, −−tcrypt−hidden, −−tcrypt−system, −−tcrypt−backup, −−veracrypt (ignored), −−disable−veracrypt, −−veracrypt−pim, −−veracrypt−query−pim, −−cipher, −−hash, −−header, −−verify−passphrase, −−timeout].

OPTIONS

−−batch−mode, **−q**

Suppresses all confirmation questions. Use with care!

If the −−verify−passphrase option is not specified, this option also switches off the passphrase verification.

−−cipher, **−c** <*cipher−spec*>

Set the cipher specification string for the *plain* device type.

For the *tcrypt* device type, it restricts checked cipher chains when looking for the header.

−−debug or **−−debug−json**

Run in debug mode with full diagnostic logs. Debug output lines are always prefixed by #.

If −−debug−json is used, additional LUKS2 JSON data structures are printed.

−−disable−veracrypt

This option can be used to disable VeraCrypt compatible mode (only TrueCrypt devices are recognized). See the *TCRYPT* section in **cryptsetup**(8) for more info.

−−dump−volume−key, −−dump−master−key (OBSOLETE alias)

Print the volume key in the displayed information. Use with care, as the volume key can be used to bypass the passphrases, see also option −−volume−key−file.

−−hash, **−h** <*hash−spec*>

Specifies the passphrase hash. Applies to *plain* and *loopaes* device types only.

For the *tcrypt* device type, it restricts the checked PBKDF2 variants when looking for the header.

−−header <*device or file storing the LUKS header*>

Use a detached (separated) metadata device or file where the LUKS header is stored. This option allows one to store the ciphertext and LUKS header on different devices.

For commands that change the LUKS header (e.g., *luksAddKey*), specify the device or file with the LUKS header directly as the LUKS device.

−−help, **−?**
Show help text and default parameters.

−−key−file, **−d** *file*
Read the passphrase from the file.

If the name given is "−", then the passphrase will be read from stdin. In this case, reading will not stop at newline characters.

See section *NOTES ON PASSPHRASE PROCESSING* in **cryptsetup**(8) for more information.

−−tcrypt−backup, **−−tcrypt−hidden**, **−−tcrypt−system**
Specify which TrueCrypt on−disk header will be used to open the device. See the *TCRYPT* section in **cryptsetup**(8) for more info.

Using a system−encrypted device with the −−tcrypt−system option requires specific settings to work as expected.

TrueCrypt/VeraCrypt supports full system encryption (only a partition table is not encrypted) or system partition encryption (only a system partition is encrypted). The metadata header then contains the offset and size of the encrypted area. Cryptsetup needs to know the specific partition offset to calculate encryption parameters. To properly map a partition, you must specify a real partition device so cryptsetup can calculate this offset.

While you can use a full device as a parameter (/dev/sdb), always prefer to specify the partition you want to map (/dev/sdb1), as only the system partition mode can be detected this way.

For mapping images (stored in a file), you can use the additional −−header option with the real partition device. If the −−header is used (and it is different from the data image), cryptsetup expects that the data image contains a snapshot of the data partition only.

If −−header is not used (or points to the same image), cryptsetup expects that the image contains a full disk (including the partition table). This can map a full encrypted area that is not directly mountable as a filesystem. Please prefer creating a loop device with partitions (**losetup −P**, see **losetup**(8) man page) and use a real partition (/dev/loopXp1) as the device parameter.

−−timeout, **−t** *seconds*
The number of seconds to wait before a timeout on passphrase input via terminal. It is relevant every time a passphrase is asked. It has no effect if used in conjunction with −−key−file.

This option is useful when the system should not stall if the user does not input a passphrase, e.g., during boot. The default is a value of 0 seconds, which means to wait forever.

−−usage
Show short option help.

−−veracrypt
This option is ignored as VeraCrypt compatible mode is supported by default.

−−veracrypt−pim, **−−veracrypt−query−pim**
Use a custom Personal Iteration Multiplier (PIM) for the VeraCrypt device. See the *TCRYPT* section in

cryptsetup(8) for more info.

−−verify−passphrase, **−y**
When interactively asking for a passphrase, ask for it twice and complain if both inputs do not match. Ignored on input from file or stdin.

−−version, **−V**
Show the program version.

REPORTING BUGS

Report bugs at cryptsetup mailing list <cryptsetup@lists.linux.dev> or in Issues project section <https://gitlab.com/cryptsetup/cryptsetup/−/issues/new>.

Please attach the output of the failed command with −−debug option added.

SEE ALSO

Cryptsetup FAQ <https://gitlab.com/cryptsetup/cryptsetup/wikis/FrequentlyAskedQuestions>

cryptsetup(8), **integritysetup**(8) and **veritysetup**(8)

CRYPTSETUP

Part of cryptsetup project <https://gitlab.com/cryptsetup/cryptsetup/>.