

Forum:[Hack Forums](#)

Thread: [Best Full Disk Encryption / File Encryption Tools](#)

T3RM1N4L - May 15, 2014, 5:58 pm

Quote: This is a thread containing the best open source FDE and File Encryption programs

Truecrypt

<http://www.truecrypt.org/>

Compatibility: Windows, Linux, OSX (note full disk encryption is only available on Windows)

Quote: Main features:

Creates a virtual encrypted disk within a file and mounts it as a real disk.

Encrypts an entire partition or storage device such as USB flash drive or hard drive.

Encrypts a partition or drive where Windows is installed (pre-boot authentication).

Encryption is automatic, real-time (on-the-fly) and transparent.

Parallelization and pipelining allow data to be read and written as fast as if the drive was not encrypted.

Encryption can be hardware-accelerated on modern processors.

Provides plausible deniability, in case an adversary forces you to reveal the password:

Hidden volume (steganography) and hidden operating system.

DiskCryptor

https://diskcryptor.net/wiki/Main_Page

Compatibility: Windows

Quote: Program Features

Support for encryption algorithm AES, Twofish, Serpent, including their combinations.

Transparent encryption of disk partitions.

Full support for dynamic disks.

Support for disk devices with large sector size (important for hardware RAID operation).

High performance, comparable to efficiency of a non-encrypted system.

Support for hardware AES acceleration:

AES-NI instruction set on new Intel CPU;

PadLock extensions on VIA processors.

Broad choice in configuration of booting an encrypted OS. Support for various multi-boot options.

Full compatibility with third party boot loaders (LILO, GRUB, etc.).

Encryption of system and bootable partitions with pre-boot authentication.

Option to place boot loader on external media and to authenticate using the key media.

Support for key files.

Full support for external storage devices.

Option to create encrypted CD and DVD disks.

Full support for encryption of external USB storage devices.

Automatic mounting of disk partitions and external storage devices.

Support for hotkeys and optional command-line interface (CLI).

Open license GNU GPLv3.

cryptsetup (LUKS)

<https://code.google.com/p/cryptsetup/>

Compatibility: Linux

Quote: With many popular Linux distros like Ubuntu there is an option to have FDE during installation, if not there are several guides on how to set it up on distros that don't have it implemented in the installer. It works differently than Windows based FDE programs and has to be set up during the installation.

Quote:What the ..?

Cryptsetup is utility used to conveniently setup disk encryption based on dm-crypt kernel module.

These include plain dm-crypt volumes, LUKS volumes, loop-AES and TrueCrypt compatible format.

Project also includes veritysetup utility used to conveniently setup dm-verity block integrity checking kernel module.

LUKS Design

LUKS is the standard for Linux hard disk encryption. By providing a standard on-disk-format, it does not only facilitate compatibility among distributions, but also provides secure management of multiple user passwords. In contrast to existing solution, LUKS stores all setup necessary setup information in the partition header, enabling the user to transport or migrate his data seamlessly.

LUKS was designed according to TKS1, a template design developed in TKS1 for secure key setup. LUKS closely reassembles the structure recommended in the TKS1 paper, but also adds meta data for cipher setup management and LUKS also supports for multiple keys/passphrases.

Why LUKS?

- compatibility via standardization,
- secure against low entropy attacks,
- support for multiple keys,
- effective passphrase revocation,
- free