

## File Systems Encryption using Linux 2.6

The 2.6 series Linux kernels implements a generic infrastructure, called device-mapper, which offers the possibility to create virtual block devices stacks, allowing overlapping several mechanisms over real file systems (e.g. concatenation, encryption, mirroring etc.).

One of the device-mapper style devices is dm-crypt, which offers transparent encryption of block devices, using cryptoapi.

Cryptoapi is an API which provides encryption algorithms, implemented at kernel level. In the future, the Linux kernel will provide support for hardware encryption devices.

To create an encrypted file system, the following steps must be followed:

- the partition or the disk which will store the encrypted file system must be populated with random data, in order to reduce data decryption possibility.
- the encrypted file system must be initialized using cryptsetup (cryptsetup create hda3 /dev/hda3)
- the cryptsetup will ask for a passphrase; this passphrase will be processed through a hash function, and the result will consists in the encryption key
- the initialization procedure will create a special device (/dev/mapper/hda3). The newly created device can be used as an ordinary partition (mounted, unmounted etc.)
- at every operating system boot time, the special device must be initialized. The system will ask for the passphrase entered at the first initialization.