dm-crypt

Device-Mapper's "crypt" target provides transparent encryption of block devices using the kernel crypto API.

Parameters: <cipher> <key> <iv_offset> <device path> <offset>

<cipher>
    Encryption cipher and an optional IV generation mode.
    (In format cipher-chainmode-ivopts:ivmode).
    Examples:
       des
       aes-cbc-essiv:sha256
       twofish-ecb

    /proc/crypto contains supported crypto modes

<key>
    Key used for encryption. It is encoded as a hexadecimal number.
    You can only use key sizes that are valid for the selected cipher.

<iv_offset>
    The IV offset is a sector count that is added to the sector number
    before creating the IV.

<device path>
    This is the device that is going to be used as backend and contains the
    encrypted data. You can specify it as a path like /dev/xxx or a device
    number <major>:<minor>.

<offset>
    Starting sector within the device where the encrypted data begins.

Example scripts

LUKS (Linux Unified Key Setup) is now the preferred way to set up disk encryption with dm-crypt using the 'cryptsetup' utility, see http://luks.endorphin.org/

[[
#!/bin/sh
Create a crypt device using dmsetup
dmsetup create crypt1 --table "0 `blockdev --getsize $1` crypt
aes-cbc-essiv:sha256 babebabebabebabebabebabebabebabe 0 $1 0"
]]

[[
#!/bin/sh
Create a crypt device using cryptsetup and LUKS header with default cipher
cryptsetup luksFormat $1
cryptsetup luksOpen $1 crypt1
]]