

# Verschlüsselung auf Geräteebene unter NetBSD

UTE vom 14. 1. 2007, Christoph Leuzinger <leuzi@trash.net>

## Wozu Verschlüsselung auf Geräteebene?

Die Verschlüsselung von Daten ist unter anderem auf mobilen Rechnern und Datenträgern wünschenswert oder notwendig, da die Gefahr des Diebstahls besondere Maßnahmen zum Schutz der Vertraulichkeit der Daten auf dem Speichermedium erfordert. Die Verschlüsselung auf Dateiebene – z. B. mit dem *GNU Privacy Guard (GnuPG)* – ist für diesen Zweck nicht immer ein geeignetes Mittel, da sich das Ver- und Entschlüsseln häufig benutzter Dateien umständlich gestaltet. Zudem besteht auch das Risiko, dass entschlüsselte Dateien nach Gebrauch nicht gelöscht werden und dass die Daten auch nach der Entfernung aus dem Dateisystem noch rekonstruierbar bleiben.

## Der Cryptographic Disk Driver

Dieses Problems nimmt sich die Verschlüsselung auf Geräteebene an. Sie ermöglicht die transparente Verschlüsselung von ganzen Partitionen mit Hilfe eines virtuellen *disk device drivers*, unter NetBSD ist dies der *Cryptographic Disk Driver (CGD)*.

Der CGD setzt auf Treiber für Massenspeichermedien wie Festplatten, Flash-Speicher, etc. auf (u. a. `wd(4)`, `sd(4)`). Ebenfalls möglich ist die Verwendung von CGD auf einer  *vnode disk*, die ein virtuelles Speichergerät mit Hilfe einer Datei simuliert (`vnd(4)`).

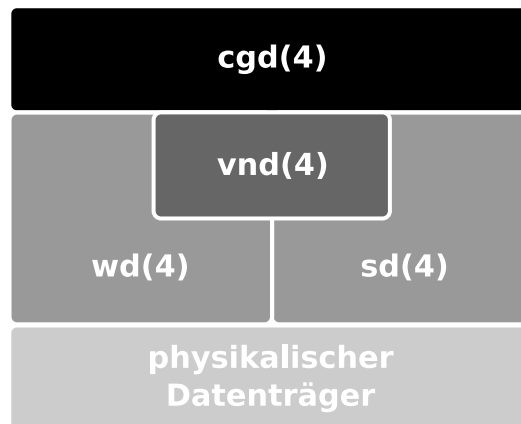


Abbildung 1: Einordnung von `cgd(4)` in die Treiberhierarchie

Der CGD bietet eine transparente Verschlüsselung an, d. h. die virtuellen Geräte, die den Zugriff auf die verschlüsselten physikalischen Geräte anbieten, können wie normale Geräte gemountet werden. Dazu finden sich die *device nodes* unter `/dev/cgdXY`.

Der CGD bietet verschiedene *Block-Ciphers* an, zur Zeit sind dies *AES*, *3DES* und *Blowfish*.

## Kommandos, Konfigurationsdateien und Devices

`cgdconfig(8)` Dieses Kommando dient der Konfiguration von CGD-Geräten und der Verwaltung der entsprechenden Konfigurationsdateien.

`/etc/cgd/` In diesem Verzeichnis werden die Dateien, die mit `cgdconfig -g` erstellt werden und die Parameter für den Kryptographie-Algorithmus und für die Schlüsselgenerierung für jedes CGD enthalten, abgelegt. Ohne die richtigen Parameter ist das Entschlüsseln einer Partition nicht möglich; es ist deshalb wichtig, dass die Parameterdateien gesichert werden.

`/etc/cgd/cgd.conf` Diese Datei dient der Konfiguration von `cgdconfig(8)`. Darin werden die `cgd`-Geräte, die physikalischen Geräten und ggf. die Parameterdateien verknüpft.

`/dev/cgd[0-3][a-p]`, `/dev/rcgd[0-3][a-p]` Die Gerätedateien (*device nodes*) für die CGD-Geräte.

## Beispiel: Verschlüsselte USB-Festplatte

### 1. Kernel mit CGD-Unterstützung bauen

Dazu muss die folgende Zeile zur Kernelkonfiguration hinzugefügt werden.

```
pseudo-device    cgd                4          # cryptographic disk devices
```

### 2. Identifizieren des Geräts

```
umass0 at uhub1 port 1 configuration 1 interface 0
umass0: LaCie LaCie HardDrive USB, rev 2.00/0.00, addr 2
umass0: using SCSI over Bulk-Only
scsibus0 at umass0: 2 targets, 1 lun per target
sd0 at scsibus0 target 0 lun 0: <SAMSUNG, MP0402H, UC10> disk fixed
sd0: 38204 MB, 77622 cyl, 16 head, 63 sec, 512 bytes/sect x 78242976 sectors
```

Die Festplatte steht in diesem Fall unter `/dev/sd0` zu Verfügung. Sie enthält lediglich eine Partition, die als verschlüsseltes CGD-Gerät verwendet werden soll.

### 3. Überschreiben der Platte mit Zufallsdaten

Dazu wird ein temporäres CGD-Gerät angelegt, mit Nullen beschrieben und anschliessend wieder entfernt.

```
# cgdconfig -g -k randomkey -o /tmp/sd0e-rnd aes-cbc
# cgdconfig cgd0 /dev/sd0e /tmp/sd0e-rnd
# dd if=/dev/zero of=/dev/rcgd0d bs=32k
# cgdconfig -u cgd0
```

### 4. Anlegen eines verschlüsselnden Devices

Wir legen eine verschlüsselte Partition auf `/dev/sd0e` an. Als Algorithmus dient *AES* mit einer Schlüssellänge von 256 Bits. Zum Verifizieren der Passwordeingabe dient das Disklabel.

```
# cgdconfig -g -V disklabel -o /etc/cgd/sd0e aes-cbc 256
```

Danach legen wir das Passwort für unsere verschlüsselte Platte fest:

```
# cgdconfig -V re-enter cgd0 /dev/sd0e
```

Anschließend kann die virtuelle Platte wie ein physikalisches Medium mit `disklabel -e -I cgd0` partitioniert und formatiert (z. B. `newfs /dev/rcgd0a`) werden. Weiter muss noch ein Eintrag in `/etc/cgd/cgd.conf` eingefügt werden:

```
cgd0 /dev/sd0e
```

Die verschlüsselten Partitionen können wie üblich in die `/etc/fstab` eingetragen werden:

```
/dev/cgd0a /crypted ffs rw,noauto,softdep 0 0
```

Soll direkt beim Booten nach dem Passwort gefragt werden, damit die Platte nach dem Systemstart zur Verfügung steht, muss zudem noch `cgd=YES` in der `/etc/rc.conf` eingetragen werden. Die CGD-Geräte können jedoch auch nach dem Systemstart, z. B. nach dem Einstecken der USB-Festplatte, verwendet werden:

```
# cgdconfig cgd0 /dev/sd0e
/dev/sd0e's passphrase:
# mount /crypted
...
# umount /crypted
# cgdconfig -u cgd0
```

## Verschlüsselung auf Geräteebene auf anderen Systemen

Neben NetBSD bietet auch FreeBSD mit *GEOM Based Disk Encryption (GBDE)* die Möglichkeit zur Verschlüsselung auf Geräteebene. Unter OpenBSD kann mit `vnconfig(8)` ein verschlüsseltes Pseudo-Device, das auf einer Datei arbeitet, angelegt werden. Linux bietet unter anderem eine Verschlüsselungsmöglichkeit mit Hilfe des *device mappers*.

Für eine ausführliche Diskussion des CGD und den Vergleich mit anderen Systemen sei der Artikel von Dowdeswell/Ioannidis, *The CryptoGraphic Disk Driver* empfohlen.

## Literatur

**Amon, Kyle:** OpenBSD Encrypted Virtual Filesystem Mini-HOWTO. [⟨URL: http://www.xs4all.nl/~hanb/documents/OpenBSDEncryptedFilesystemHOWTO.html⟩](http://www.xs4all.nl/~hanb/documents/OpenBSDEncryptedFilesystemHOWTO.html)

**Dowdeswell, Roland C./Ioannidis, John:** The CryptoGraphic Disk Driver. [⟨URL: http://www.imrryr.org/~elric/cgd/cgd.pdf⟩](http://www.imrryr.org/~elric/cgd/cgd.pdf)

**Green, Lucky:** Das FreeBSD-Handbuch: Partitionen verschlüsseln. [⟨URL: http://www.freebsd.org/doc/de/books/handbook/disks-encrypting.html⟩](http://www.freebsd.org/doc/de/books/handbook/disks-encrypting.html)

**Kamp, Poul-Henning:** GBDE - GEOM Based Disk Encryption. [⟨URL: http://phk.freebsd.dk/pubs/bsdcon-03.gbde.paper.pdf⟩](http://phk.freebsd.dk/pubs/bsdcon-03.gbde.paper.pdf)

**Lavigne, Dru:** BSD Hacks. O'Reilly, 2005, S. 285–291

**NetBSD Developers, The:** The NetBSD Guide: The cryptographic device driver (CGD). [⟨URL: http://www.netbsd.org/guide/en/chap-cgd.html⟩](http://www.netbsd.org/guide/en/chap-cgd.html)

**Saout, Christophe:** dm-crypt: a device-mapper crypto target. (URL: <http://www.saout.de/misc/dm-crypt/>)

**Schumacher, Stefan:** Verschlüsselte Dateisysteme für NetBSD. (URL: [http://net-tex.dnsalias.org/~stefan/nt/netbsd/advocacy/guug-uptimes-cgd\\_cfs.pdf](http://net-tex.dnsalias.org/~stefan/nt/netbsd/advocacy/guug-uptimes-cgd_cfs.pdf))

**Wikipedia:** Disk encryption software. (URL: [http://en.wikipedia.org/wiki/Disk\\_encryption\\_software](http://en.wikipedia.org/wiki/Disk_encryption_software))