

NAME

glxsb - Geode LX Security Block crypto accelerator

SYNOPSIS

To compile this driver into the kernel, place the following lines in your kernel configuration file:

```
device crypto
device glxsb
```

Alternatively, to load the driver as a module at boot time, place the following line in loader.conf(5):

```
glxsb_load="YES"
```

DESCRIPTION

The **glxsb** driver supports the security block of the Geode LX series processors. The Geode LX is a member of the AMD Geode family of integrated x86 system chips.

Driven by periodic checks for available data from the generator, **glxsb** supplies entropy to the random(4) driver for common usage.

glxsb also supports acceleration of AES-128-CBC operations for crypto(4). It also registers itself to accelerate other HMAC algorithms, although there is no hardware acceleration for those algorithms. This is only needed so **glxsb** can work with ipsec(4).

CAVEAT

The crypto(9) framework will fail to open the crypto session on the device if the AES key's length is != 128 bits. This prevents the use of the **glxsb** device driver with AES keys of length != 128 bits.

SEE ALSO

crypto(4), intro(4), ipsec(4), pci(4), random(4), crypto(7), crypto(9)

HISTORY

The **glxsb** device driver first appeared in OpenBSD 4.1. The **glxsb** device driver was imported into FreeBSD 7.1.

AUTHORS

The **glxsb** device driver was written for OpenBSD by Tom Cosgrove. It was ported to FreeBSD by Patrick Lamaiziere <patfbsd@davenulle.org>.