NAME

hifn - Hifn 7751/7951/7811/7955/7956 crypto accelerator

SYNOPSIS

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

```
device crypto
device cryptodev
device hifn
```

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

```
hifn_load="YES"
```

DESCRIPTION

The **hifn** driver supports various cards containing the Hifn 7751, 7951, 7811, 7955, and 7956 chipsets.

The **hifn** driver registers itself to accelerate AES (7955 and 7956 only), SHA1, and SHA1-HMAC operations for ipsec(4) and crypto(4).

The Hifn 7951, 7811, 7955, and 7956 will also supply data to the kernel random(4) subsystem.

HARDWARE

The **hifn** driver supports various cards containing the Hifn 7751, 7951, 7811, 7955, and 7956 chipsets, such as:

Invertex AEON — No longer being made. Came as 128KB SRAM model, or 2MB DRAM model.

Hifn 7751 — Reference board with 512KB SRAM.

PowerCrypt — Comes with 512KB SRAM.

XL-Crypt — Only board based on 7811 (which is faster than 7751 and has a random number generator).

NetSec 7751 — Supports the most IPsec sessions, with 1MB SRAM.

Soekris Engineering vpn1201 and vpn1211
See *http://www.soekris.com/*. Contains a 7951 and supports symmetric and

random number operations.

Soekris Engineering vpn1401 and vpn1411
See *http://www.soekris.com/*. Contains a 7955 and supports symmetric and random number operations.

SEE ALSO

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

HISTORY

The **hifn** device driver appeared in OpenBSD 2.7. The **hifn** device driver was imported to FreeBSD 5.0.

CAVEATS

The Hifn 9751 shares the same PCI ID. This chip is basically a 7751, but with the cryptographic functions missing. Instead, the 9751 is only capable of doing compression. Since we do not currently attempt to use any of these chips to do compression, the 9751-based cards are not useful.

Support for the 7955 and 7956 is incomplete; the asymmetric crypto facilities are to be added and the performance is suboptimal.

BUGS

The 7751 chip starts out at initialization by only supporting compression. A proprietary algorithm, which has been reverse engineered, is required to unlock the cryptographic functionality of the chip. It is possible for vendors to make boards which have a lock ID not known to the driver, but all vendors currently just use the obvious ID which is 13 bytes of 0.