NAME

safe - SafeNet crypto accelerator

SYNOPSIS

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

```
device crypto
device cryptodev
device safe
```

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

```
safe_load="YES"
```

sysctl *hw.safe.debug*
sysctl *hw.safe.dump*
sysctl *hw.safe.rnginterval*
sysctl *hw.safe.rngbufsize*
sysctl *hw.safe.rngmaxalarm*

DESCRIPTION

The **safe** driver supports cards containing SafeNet crypto accelerator chips.

The **safe** driver registers itself to accelerate AES, SHA1-HMAC, and NULL operations for ipsec(4) and crypto(4).

On all models, the driver registers itself to provide random data to the random(4) subsystem. Periodically the driver will poll the hardware RNG and retrieve data for use by the system. If the driver detects that the hardware RNG is resonating with any local signal, it will reset the oscillators that generate random data. Three sysctl(8) settings control this procedure: *hw.safe.rnginterval* specifies the time, in seconds, between polling operations, *hw.safe.rngbufsize* specifies the number of 32-bit words to retrieve on each poll, and *hw.safe.rngmaxalarm* specifies the threshold for resetting the oscillators.

When the driver is compiled with SAFE_DEBUG defined, two sysctl(8) variables are provided for debugging purposes: *hw.safe.debug* can be set to a non-zero value to enable debugging messages to be sent to the console for each cryptographic operation, *hw.safe.dump* is a write-only variable that can be used to force driver state to be sent to the console. Set this variable to "ring" to dump the current state of the descriptor ring, to "dma" to dump the hardware DMA registers, or to "int" to dump the hardware interrupt registers.

HARDWARE

The **safe** driver supports cards containing any of the following chips:

SafeNet 1141 The original chipset. Supports DES, Triple-DES, AES, MD5, and SHA-1 symmetric crypto operations, RNG, public key operations, and full IPsec packet processing.

SafeNet 1741 A faster version of the 1141.

SEE ALSO

crypt(3), crypto(4), intro(4), ipsec(4), random(4), crypto(7), crypto(9)

BUGS

Public key support is not implemented.