NAME

tpm **-** Trusted Platform Module

SYNOPSIS

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

```
device tpm
```

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

```
tpm_load="YES"
```

In */boot/device.hints*:

```
hint.tpm.0.at="isa"
hint.tpm.0.maddr="0xfed40000"
hint.tpm.0.msize="0x5000"
hint.tpm.1.at="isa"
hint.tpm.1.maddr="0xfed40000"
hint.tpm.1.msize="0x1000"
```

DESCRIPTION

The **tpm** driver provides support for various trusted platform modules (TPM) that can store cryptographic keys.

Supported modules:

- Atmel 97SC3203
- Broadcom BCM0102
- Infineon IFX SLD 9630 TT 1.1 and IFX SLB 9635 TT 1.2
- Intel INTC0102
- Sinosun SNS SSX35
- STM ST19WP18
- Winbond WEC WPCT200

The driver can be configured to use an IRQ by providing a free ISA interrupt vector in */boot/device.hints*.

SEE ALSO

intro(4), device.hints(5), config(8)

The homepage of the BSSSD project, which developed the original **tpm** driver: **http://bsssd.sourceforge.net/**.

TPM main specification can be found at: **https://trustedcomputinggroup.org/resource/tpm-main-specification/**.

STANDARDS

TPM Main Specification Level 2 Version 1.2:

- ISO/IEC, *11889-1:2009, Information technology -- Trusted Platform Module -- Part 1: Overview*, https://www.iso.org/standard/50970.html.

- ISO/IEC, *11889-2:2009, Information technology -- Trusted Platform Module -- Part 2: Design principles*, https://www.iso.org/standard/50971.html.

- ISO/IEC, *11889-3:2009, Information technology -- Trusted Platform Module -- Part 3: Structures*, https://www.iso.org/standard/50972.html.

HISTORY

The **tpm** driver first appeared in FreeBSD 8.2 and was later added to OpenBSD 6.1.

AUTHORS

The **tpm** driver was written by Michael Shalayeff and Hans-Joerg Hoexer.