NAME

rndtest - FIPS 140-2 random number generator test monitor

SYNOPSIS

device rndtest

DESCRIPTION

The **rndtest** driver "hooks up" to hardware crypto devices to monitor the entropy data passed to the random(4) subsystem. This data is periodically tested for FIPS 140-2 compliance and statistics are collected. If the harvested entropy fails any of the FIPS test suite, then it is discarded and testing is continuously applied until "good data" is received from the device. Failures are optionally reported on the console.

SEE ALSO

crypto(4), hifn(4), random(4), safe(4), crypto(9)

HISTORY

The idea for this and the original code came from Jason L. Wright. The **rndtest** device driver first appeared in FreeBSD 5.0.

BUGS

Crypto device drivers must be compiled specially to make use of this driver; this should not be necessary. This feature might better be integrated into the random(4) subsystem where it can be applied to devices that claim to supply "pure entropy".