NAME

qat_c2xxx - Intel QuickAssist Technology (QAT) driver for Atom C2000 chipsets

SYNOPSIS

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

```
device crypto
device cryptodev
device qat
```

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

```
qat_c2xxx_load="YES"
qat_c2xxxfw_load="YES"
```

DESCRIPTION

The **qat_c2xxx** driver implements crypto(4) support for some of the cryptographic acceleration functions of the Intel QuickAssist (QAT) device found on Atom C2000 devices. QAT devices are enumerated through PCIe and are thus visible in pciconf(8) output.

The **qat_c2xxx** driver can accelerate AES in CBC, CTR, and GCM modes, and can perform authenticated encryption combining the CBC, and CTR modes with SHA1-HMAC and SHA2-HMAC. The **qat_c2xxx** driver can also compute SHA1 and SHA2 digests. The implementation of AES-GCM has a firmware-imposed constraint that the length of any additional authenticated data (AAD) must not exceed 240 bytes. The driver thus rejects crypto(9) requests that do not satisfy this constraint.

SEE ALSO

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

HISTORY

The **qat_c2xxx** driver first appeared in FreeBSD 13.0.

AUTHORS

The **qat_c2xxx** driver was written for NetBSD by Hikaru Abe <*hikaru@iij.ad.jp*>.
Mark Johnston <*markj@FreeBSD.org*> ported the driver to FreeBSD.

BUGS

Some Atom C2000 QAT devices have two acceleration engines instead of one. The **qat_c2xxx** driver currently misbehaves when both are enabled and thus does not enable the second acceleration engine if one is present.