Manual Build of OpenSSL with Cryptodev Engine Support

Downloading OpenSSL from repo :

```
user@localhost:~$ git clone -b openssl-3.0.2 --single-branch
https://source.codeaurora.org/external/qoriq/qoriq-components/openssl
```

Build openssl with cryptodev support:

```
user@localhost:~$ ./Configure enable-devcryptoeng -I./include --
prefix=/usr/local/openssl3 --openssldir=lib/ssl linux-aarch64 shared

user@localhost:~$ sudo make

user@localhost:~$ sudo make install
```

After installation, verify that the binary is linking with the correct share library from /usr/local/openssl3/lib :

```
user@localhost:~$ ldd /usr/local/openssl3/bin/openssl
```

Once Again Check the Linkers' Path & Also OpenSSL working or not

```
user@localhost:~$ sudo vim /etc/ld.so.conf

# libc default configuration

/usr/local/openssl3/lib

# Multiarch support

/usr/local/lib/aarch64-linux-gnu

/lib/aarch64-linux-gnu

/usr/lib/aarch64-linux-gnu

/usr/lib/aarch64-linux-gnu/libfakeroot

user@localhost:~$ sudo ldconfig

user@localhost:~$ sudo vim /etc/environment

PATH="/usr/local/sbin:/usr/local/openssl3/bin/:/usr/local/bin:/usr/sbin:/u
sr/bin:/sbin:/bin:/usr/games:/usr/local/games"

user@localhost:~$ source /etc/environment
```

Now check the version of OpenSSL:

```
user@localhost:~$ openssl version -a

OpenSSL 3.0.2 15 Mar 2022 (Library: OpenSSL 3.0.2 15 Mar 2022)

Successfully installed openssl 3.0.2 in NXP board
```

Now CAAM hardware will offloaded into OpenSSL:

```
user@localhost:~$ sudo modprobe caam

[sudo] password for user:

user@localhost:~$ [  298.601056] caam_jr 1730000.jr: failed to flush job
ring 2

user@localhost:~$ sudo modprobe cryptodev

user@localhost:~$ ls /dev/crypto

/dev/crypto

user@localhost:~$ openssl engine devcrypto

(devcrypto) /dev/crypto engine

C0269197FFFF0000:error:1280006A:DSO support routines:dlfcn_bind_func:could
not bind to the requested symbol
name:crypto/dso/dso_dlfcn.c:188:symname(Ed

C0269197FFFF0000:error:1280006A:DSO support routines:DSO_bind_func:could
not bind to the requested symbol name:crypto/dso/dso_lib.c:17
```

Verify the CAAM offloading:

Hardware operations can be monitored with the interrupt counters for CAAM JR and QI (DPAA1 and DPAA2) interfaces.Generate keys with OpenSSL

Generate public/private keys using openssl command:

```
user@localhost:~/key$ openssl genpkey -algorithm RSA -out dev.key -pkeyopt
rsa_keygen_bits:2048 -pkeyopt rsa_keygen_pubexp:65537 -engine devcrypto

Engine "devcrypto" set.

Segmentation fault

user@localhost:~/key$ cat /proc/interrupts | grep jr

78:   722    0          0          0     GICv2 103 Level     1710000.jr

79:   526    0          0          0     GICv2 104 Level     1720000.jr

80:   0      0          0          0     GICv2 105 Level     fsl-jr0
```

Generate public key certificate using openssl command

```
user@localhost:~/key$ openssl req -batch -new -x509 -key dev.key -out
dev.crt

Engine "devcrypto" set.

Segmentation fault

user@localhost:~/key$ ls

dev.crt  dev.key

user@localhost:~/key$ cat /proc/interrupts | grep jr

78:        768          0          0          0     GICv2 103 Level
1710000.jr

79:        571          0          0          0     GICv2 104 Level
1720000.jr

80:          0          0          0          0     GICv2 105 Level
fsl-jr0
```

View public key

```
user@localhost:~/key$ openssl rsa -in dev.key -pubout -engine devcrypto

Engine "devcrypto" set.

writing RSA key

-----BEGIN PUBLIC KEY-----

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnR/+DZi/OhFiAFJEjU8c

pEEViraR2dsty/6qcX//0gFS8jy+Eek/a4kO995TqDC92tlLkmkGQvtdXZbqfIkx

doFzBqxRZorar+GrYW8vbwLMpeVwCh/ioPcIK852rJXRrV5nUJ8qmgJ3774r15SK

zzEaihUbKJFS0sA2fCDwYXtawJzjxzkn6kVHBskpC5PmU7wty1N2ohat+abCuWXF

UQyq2K4vuN2winu+2GRStRQ67pHT0xMyuRq54Zm/NGHK3wKAxlJ+gOp/LfyO2ONn

cKCywx5zCpaV8aEFBq9vVjtIVMRxSkE62h2JJDI/RGsU5u01LbucvtezxJw0Uxq7

vwIDAQAB

-----END PUBLIC KEY-----

user@localhost:~/key$
```

RSA Key pair generation

```
user@localhost:~/key$ cat /proc/interrupts | grep jr
78:  1707     0          0          0     GICv2 103 Level     1710000.jr
79:  1392     0          0          0     GICv2 104 Level     1720000.jr
80:     0     0          0          0     GICv2 105 Level     fsl-jr0
user@localhost:~/key$ openssl genrsa -engine devcrypto -out rsa-
private.key 4096
Engine "devcrypto" set.
Segmentation fault
user@localhost:~/key$ cat /proc/interrupts | grep jr
78:  3055     0          0          0     GICv2 103 Level     1710000.jr
79:  2177     0          0          0     GICv2 104 Level     1720000.jr
80:     0     0          0          0     GICv2 105 Level     fsl-jr0
user@localhost:~/key$ openssl rsa -engine devcrypto -in rsa-private.key -
out rsa-public.key -pubout -outform PEM
Engine "devcrypto" set.
writing RSA key
user@localhost:~/key$ cat /proc/interrupts | grep jr
78:  3055     0          0          0     GICv2 103 Level     1710000.jr
79:  2177     0          0          0     GICv2 104 Level     1720000.jr
80:     0     0          0          0     GICv2 105 Level     fsl-jr0
```

EC key pair generation(ECDSA and ECDH)

secp256k1

```
user@localhost:~/key$ openssl ecparam -name secp256k1 -genkey -noout -out
ec-secp256k1-priv-key.key -engine devcrypto
Engine "devcrypto" set.
Segmentation fault
```

```
user@localhost:~/key$ openssl ec -in ec-secp256k1-priv-key.key -pubout >
ec-secp256k1-pub-key.key -engine devcrypto

Engine "devcrypto" set.

read EC key

writing EC key

user@localhost:~/key$ cat /proc/interrupts | grep jr

78:   4662     0          0          0     GICv2 103 Level     1710000.jr

79:   3102     0          0          0     GICv2 104 Level     1720000.jr

80:      0     0          0          0     GICv2 105 Level     fsl-jr0

user@localhost:~/key$
```

secp384r1

```
user@localhost:~/key$ openssl ecparam -genkey -name secp384r1 -noout -out
ec384-pri-key.key -engine devcrypto

Engine "devcrypto" set.

Segmentation fault

user@localhost:~/key$ openssl ec -in ec384-pri-key.key -pubout >
secp384r1-pub-key.key -engine devcrypto

Engine "devcrypto" set.

read EC key

writing EC key

user@localhost:~/key$ cat /proc/interrupts | grep jr

78:   4694     0          0          0     GICv2 103 Level     1710000.jr

79:   3131     0          0          0     GICv2 104 Level     1720000.jr

80:      0     0          0          0     GICv2 105 Level     fsl-jr0
```

secp521r1

```
user@localhost:~/key$ openssl ecparam -genkey -name secp521r1 -noout -out
ec512-key-pair.key -engine devcrypto

Engine "devcrypto" set.

Segmentation fault
```

```
user@localhost:~/key$ openssl ec -in ec512-key-pair.key  -pubout > ec512-
pub-key.key -engine devcrypto

Engine "devcrypto" set.

read EC key

writing EC key

user@localhost:~/key$ cat /proc/interrupts | grep jr

78: 4733     0          0          0     GICv2 103 Level     1710000.jr

79: 3160     0          0          0     GICv2 104 Level     1720000.jr

80:    0     0          0          0     GICv2 105 Level     fsl-jr0

user@localhost:~/key$
```

AES [aes-256-cfb]

```
user@localhost:~/key$ openssl enc -aes-256-cfb -k secret -P -md sha1 -
engine devcrypto

Engine "devcrypto" set.

*** WARNING : deprecated key derivation used.

Using -iter or -pbkdf2 would be better.

Error setting cipher AES-256-CFB

C0B69290FFFF0000:error:13000092:engine
routines:ENGINE_get_cipher:unimplemented
cipher:crypto/engine/tb_cipher.c:78:

C0B69290FFFF0000:error:03000086:digital envelope
routines:evp_cipher_init_internal:initialization
error:crypto/evp/evp_enc.c:277:

Segmentation fault

user@localhost:~/key$ cat /proc/interrupts | grep jr

78:    4760    0          0          0     GICv2 103 Level     1710000.jr

79:    3184    0          0          0     GICv2 104 Level     1720000.jr

80:       0    0          0          0     GICv2 105 Level     fsl-jr0
```

Rand bit generation

```
user@localhost:~/key$ openssl rand -engine devcrypto 256 > sym_keyfile.key
Engine "devcrypto" set.
Segmentation fault
user@localhost:~/key$ cat /proc/interrupts | grep jr
78:       4814  0         0          0     GICv2 103 Level     1710000.jr
79:       3232  0         0          0     GICv2 104 Level     1720000.jr
80:          0  0          0          0     GICv2 105 Level     fsl-jr0
```

AES [aes-256-cbc]

```
user@localhost:~/key$ openssl enc -aes-256-user@localhost:~/key$ openssl
enc -aes-256-cbc -k secret -P -md sha1 -engine devcrypto
Engine "devcrypto" set.
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
salt=40F1049AE04939DD
key=0DDBD8C52848B6D51260F0D380E0FBFECDDD221CBCF808D306E8B1BB5F81B1F3
iv =29DA9279D43F56C292FF7F36FB0C292A
Segmentation fault
user@localhost:~/key$ cat /proc/interrupts | grep jr
78:  4840    0          0          0     GICv2 103 Level     1710000.jr
79:  3256    0          0          0     GICv2 104 Level     1720000.jr
80:     0    0          0          0     GICv2 105 Level     fsl-jr0
user@localhost:~/key$ls
ec384-pri-key.key       ec512-key-pair.key      ec512-pub-key.key
ec-secp256k1-priv-key.key ec-secp256k1-pub-key.key    rsa-private.key
rsa-public.key    rsa-public-key.pem      secp384r1-pub-key.key
sym_keyfile.key
```