



# DPDK

DATA PLANE DEVELOPMENT KIT

## **Crypto Device Drivers**

*Release 18.08.0*

August 31, 2018

## CONTENTS

<b>1</b>	<b>Crypto Device Supported Functionality Matrices</b>	<b>1</b>
1.1	Supported Feature Flags . . . . .	2
1.2	Supported Cipher Algorithms . . . . .	5
1.3	Supported Authentication Algorithms . . . . .	7
1.4	Supported AEAD Algorithms . . . . .	8
<b>2</b>	<b>AESN-NI Multi Buffer Crypto Poll Mode Driver</b>	<b>9</b>
2.1	Features . . . . .	9
2.2	Limitations . . . . .	10
2.3	Installation . . . . .	10
2.4	Initialization . . . . .	10
2.5	Extra notes . . . . .	11
<b>3</b>	<b>AES-NI GCM Crypto Poll Mode Driver</b>	<b>12</b>
3.1	Features . . . . .	12
3.2	Limitations . . . . .	12
3.3	Installation . . . . .	12
3.4	Initialization . . . . .	13
<b>4</b>	<b>ARMv8 Crypto Poll Mode Driver</b>	<b>14</b>
4.1	Features . . . . .	14
4.2	Installation . . . . .	14
4.3	Initialization . . . . .	15
4.4	Limitations . . . . .	15
<b>5</b>	<b>AMD CCP Poll Mode Driver</b>	<b>16</b>
5.1	Features . . . . .	16
5.2	Installation . . . . .	17
5.3	Initialization . . . . .	17
5.4	Limitations . . . . .	18
<b>6</b>	<b>NXP DPAA2 CAAM (DPAA2_SEC)</b>	<b>19</b>
6.1	Architecture . . . . .	19
6.2	Implementation . . . . .	19
6.3	Features . . . . .	20
6.4	Supported DPAA2 SoCs . . . . .	21
6.5	Whitelisting & Blacklisting . . . . .	21
6.6	Limitations . . . . .	21
6.7	Prerequisites . . . . .	21
6.8	Pre-Installation Configuration . . . . .	22

6.9	Installations . . . . .	22
6.10	Enabling logs . . . . .	22
<b>7</b>	<b>NXP DPAA CAAM (DPAA_SEC)</b>	<b>23</b>
7.1	Architecture . . . . .	23
7.2	Implementation . . . . .	23
7.3	Features . . . . .	23
7.4	Supported DPAA SoCs . . . . .	24
7.5	Whitelisting & Blacklisting . . . . .	24
7.6	Limitations . . . . .	24
7.7	Prerequisites . . . . .	25
7.8	Pre-Installation Configuration . . . . .	25
7.9	Installations . . . . .	25
7.10	Enabling logs . . . . .	25
<b>8</b>	<b>KASUMI Crypto Poll Mode Driver</b>	<b>27</b>
8.1	Features . . . . .	27
8.2	Limitations . . . . .	27
8.3	Installation . . . . .	27
8.4	Initialization . . . . .	28
8.5	Extra notes on KASUMI F9 . . . . .	28
<b>9</b>	<b>OpenSSL Crypto Poll Mode Driver</b>	<b>29</b>
9.1	Features . . . . .	29
9.2	Installation . . . . .	30
9.3	Initialization . . . . .	30
9.4	Limitations . . . . .	30
<b>10</b>	<b>MVSAM Crypto Poll Mode Driver</b>	<b>32</b>
10.1	Features . . . . .	32
10.2	Limitations . . . . .	33
10.3	Installation . . . . .	33
10.4	Initialization . . . . .	33
<b>11</b>	<b>Null Crypto Poll Mode Driver</b>	<b>35</b>
11.1	Features . . . . .	35
11.2	Limitations . . . . .	35
11.3	Installation . . . . .	35
11.4	Initialization . . . . .	36
<b>12</b>	<b>Cryptodev Scheduler Poll Mode Driver Library</b>	<b>37</b>
12.1	Limitations . . . . .	37
12.2	Installation . . . . .	38
12.3	Initialization . . . . .	38
12.4	Cryptodev Scheduler Modes Overview . . . . .	39
<b>13</b>	<b>SNOW 3G Crypto Poll Mode Driver</b>	<b>41</b>
13.1	Features . . . . .	41
13.2	Limitations . . . . .	41
13.3	Installation . . . . .	41
13.4	Initialization . . . . .	42
<b>14</b>	<b>Intel(R) QuickAssist (QAT) Crypto Poll Mode Driver</b>	<b>43</b>

14.1	Features	43
14.2	Limitations	44
14.3	Extra notes on KASUMI F9	44
14.4	Building the DPDK QAT cryptodev PMD	45
14.5	Dependency on the QAT kernel driver	45
14.6	Device and driver naming	45
14.7	Available kernel drivers	46
14.8	Installation using kernel.org driver	46
14.9	Installation using 01.org QAT driver	47
14.10	Binding the available VFs to the DPDK UIO driver	49
14.11	Debugging	50
<b>15</b>	<b>Virtio Crypto Poll Mode Driver</b>	<b>51</b>
15.1	Features	51
15.2	Limitations	51
15.3	Virtio crypto PMD Rx/Tx Callbacks	51
15.4	Installation	52
15.5	Tests	52
<b>16</b>	<b>ZUC Crypto Poll Mode Driver</b>	<b>53</b>
16.1	Features	53
16.2	Limitations	53
16.3	Installation	53
16.4	Initialization	54



## CHAPTER

## ONE

## CRYPTO DEVICE SUPPORTED FUNCTIONALITY MATRICES

## 1.1 Supported Feature Flags

Table 1.1: Features availability in crypto drivers

Feature	aes ni_ gcm	aes ni_ mb	arm v8	ccp	dpaa2_ sec	dpaa_ sec	kasumi	mvsa	nu	openssl	qat	snow3g	virtio	zuc
Symmetric crypto	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Asymmetric crypto										Y				
Sym operation chaining	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
HW Accelerated				Y	Y	Y					Y			
Protocol offload					Y	Y								
CPU SSE	Y	Y												
CPU AVX	Y	Y												
CPU AVX2	Y	Y												
CPU AVX512		Y												
CPU AESNI	Y	Y												
CPU NEON			Y											
CPU ARM CE			Y											
1.1. Supported Feature Flags					Y	Y			Y		Y			2
Place SGL														
OOP					Y	Y					Y			

**Note:**

- “In Place SGL” feature flag stands for “In place Scatter-gather list”, which means that an input buffer can consist of multiple segments, being the operation in-place (input address = output address).
  - “OOP SGL In SGL Out” feature flag stands for “Out-of-place Scatter-gather list Input, Scatter-gather list Output”, which means pmd supports different scatter-gather styled input and output buffers (i.e. both can consists of multiple segments).
  - “OOP SGL In LB Out” feature flag stands for “Out-of-place Scatter-gather list Input, Linear Buffers Output”, which means PMD supports input from scatter-gathered styled buffers, outputting linear buffers (i.e. single segment).
  - “OOP LB In SGL Out” feature flag stands for “Out-of-place Linear Buffers Input, Scatter-gather list Output”, which means PMD supports input from linear buffer, outputting scatter-gathered styled buffers.
  - “OOP LB In LB Out” feature flag stands for “Out-of-place Linear Buffers Input, Scatter-gather list Output”, which means that Out-of-place operation is supported, with linear input and output buffers.
-





## 1.2 Supported Cipher Algorithms

Table 1.2: Cipher algorithms in crypto drivers

Ci- pher algo- rithm	a e s n i _ g c m	a e s n i _ m b	a r m v 8	c p	d p a a 2 _ s e c	d p a a _ s e c	k a s u m i	m v s a m	n u l l	o p e n s s l	q a t	s n o w 3 g	v i r t i o	z u c
NULL									Y		Y			
AES CBC (128)		Y	Y	Y	Y	Y		Y		Y	Y		Y	
AES CBC (192)		Y		Y	Y	Y		Y		Y	Y		Y	
AES CBC (256)		Y		Y	Y	Y		Y		Y	Y		Y	
AES ECB (128)				Y										
AES ECB (192)				Y										
AES ECB (256)				Y										
AES CTR (128)		Y		Y	Y	Y		Y		Y	Y			
AES CTR (192)		Y		Y	Y	Y		Y		Y	Y			
AES CTR (256)		Y		Y	Y	Y		Y		Y	Y			
AES DOC- SIS BPI		Y									Y			
3DES CBC		Y		Y	Y	Y		Y		Y	Y			
3DES CTR								Y		Y	Y			
DES CBC		Y									Y			
DES DOC- SIS BPI		Y								Y	Y			
SNOW3G UEA2											Y	Y		
12A-Supported Cipher Algorithms							Y				Y			5
SUMI F8														
ZUC											Y			Y



## 1.3 Supported Authentication Algorithms

Table 1.3: Authentication algorithms in crypto drivers

Authentication algorithm	aesni_gcm	aesni_mb	armv8	ccp	dpaa2_sec	dpaa_sec	kaumi	mvsa	null	openssl	qat	snow3g	virtio	zuc
NULL									Y		Y			
MD5								Y		Y				
MD5 HMAC		Y		Y	Y	Y		Y		Y	Y			
SHA1				Y				Y		Y				
SHA1 HMAC		Y	Y	Y	Y	Y		Y		Y	Y		Y	
SHA224				Y						Y				
SHA224 HMAC		Y		Y	Y	Y				Y	Y			
SHA256				Y				Y		Y				
SHA256 HMAC		Y	Y	Y	Y	Y		Y		Y	Y			
SHA384				Y				Y		Y				
SHA384 HMAC		Y		Y	Y	Y		Y		Y	Y			
SHA512				Y				Y		Y				
SHA512 HMAC		Y		Y	Y	Y		Y		Y	Y			
AES XCBC MAC		Y									Y			
AES GMAC	Y							Y		Y	Y			
SNOW3G UIA2											Y	Y		
KA-SUMI F9							Y				Y			
ZUC EIA3											Y			Y
AES CMAC (128)		Y		Y										
AES CMAC (192)				Y										
AES CMAC (256)				Y										
SHA3_224				Y										
SHA3_224 HMAC				Y										
SHA3_256				Y										
SHA3_256 HMAC				Y										
SHA3_384				Y										

## 1.4 Supported AEAD Algorithms

Table 1.4: AEAD algorithms in crypto drivers

AEAD algo- rithm	aes ni_ gcm	aes ni_ mb	arm v8	ccp	dpa a2_ sec	dpa aa_ sec	kasu mi	mvsa m	nu ll	open ssl	qat	snow 3g	virtio	zuc
AES GCM (128)	Y			Y	Y	Y		Y		Y	Y			
AES GCM (192)	Y			Y	Y	Y				Y	Y			
AES GCM (256)	Y			Y	Y	Y				Y	Y			
AES CCM (128)		Y								Y				
AES CCM (192)										Y				
AES CCM (256)										Y				

## AESN-NI MULTI BUFFER CRYPTO POLL MODE DRIVER

The AESNI MB PMD (`librte_pmd_aesni_mb`) provides poll mode crypto driver support for utilizing Intel multi buffer library, see the white paper [Fast Multi-buffer IPsec Implementations on Intel® Architecture Processors](#).

The AES-NI MB PMD has current only been tested on Fedora 21 64-bit with gcc.

### 2.1 Features

AESNI MB PMD has support for:

Cipher algorithms:

- `RTE_CRYPTO_CIPHER_AES128_CBC`
- `RTE_CRYPTO_CIPHER_AES192_CBC`
- `RTE_CRYPTO_CIPHER_AES256_CBC`
- `RTE_CRYPTO_CIPHER_AES128_CTR`
- `RTE_CRYPTO_CIPHER_AES192_CTR`
- `RTE_CRYPTO_CIPHER_AES256_CTR`
- `RTE_CRYPTO_CIPHER_AES_DOCSISBPI`
- `RTE_CRYPTO_CIPHER_DES_CBC`
- `RTE_CRYPTO_CIPHER_3DES_CBC`
- `RTE_CRYPTO_CIPHER_DES_DOCSISBPI`

Hash algorithms:

- `RTE_CRYPTO_HASH_MD5_HMAC`
- `RTE_CRYPTO_HASH_SHA1_HMAC`
- `RTE_CRYPTO_HASH_SHA224_HMAC`
- `RTE_CRYPTO_HASH_SHA256_HMAC`
- `RTE_CRYPTO_HASH_SHA384_HMAC`
- `RTE_CRYPTO_HASH_SHA512_HMAC`
- `RTE_CRYPTO_HASH_AES_XCBC_HMAC`

- RTE\_CRYPT\_HASH\_AES\_CMAC

AEAD algorithms:

- RTE\_CRYPT\_AEAD\_AES\_CCM

## 2.2 Limitations

- Chained mbufs are not supported.
- Only in-place is currently supported (destination address is the same as source address).

## 2.3 Installation

To build DPDK with the AESNI\_MB\_PMD the user is required to download the multi-buffer library from [here](https://github.com/01org/intel-ipsec-mb/archive/v0.50.zip) and compile it on their user system before building DPDK. The latest version of the library supported by this PMD is v0.50, which can be downloaded from <https://github.com/01org/intel-ipsec-mb/archive/v0.50.zip>.

```
make
make install
```

As a reference, the following table shows a mapping between the past DPDK versions and the Multi-Buffer library version supported by them:

Table 2.1: DPDK and Multi-Buffer library version compatibility

DPDK version	Multi-buffer library version
2.2 - 16.11	0.43 - 0.44
17.02	0.44
17.05 - 17.08	0.45 - 0.48
17.11	0.47 - 0.48
18.02	0.48
18.05+	0.49+

## 2.4 Initialization

In order to enable this virtual crypto PMD, user must:

- Build the multi buffer library (explained in Installation section).
- Set CONFIG\_RTE\_LIBRTE\_PMD\_AESNI\_MB=y in config/common\_base.

To use the PMD in an application, user must:

- Call `rte_vdev_init("crypto_aesni_mb")` within the application.
- Use `-vdev="crypto_aesni_mb"` in the EAL options, which will call `rte_vdev_init()` internally.

The following parameters (all optional) can be provided in the previous two calls:

- `socket_id`: Specify the socket where the memory for the device is going to be allocated (by default, `socket_id` will be the socket where the core that is creating the PMD is running on).
- `max_nb_queue_pairs`: Specify the maximum number of queue pairs in the device (8 by default).
- `max_nb_sessions`: Specify the maximum number of sessions that can be created (2048 by default).

Example:

```
./l2fwd-crypto -l 1 -n 4 --vdev="crypto_aesni_mb,socket_id=0,max_nb_sessions=128" \  
-- -p 1 --cdev SW --chain CIPHER_HASH --cipher_algo "aes-cbc" --auth_algo "sha1-hmac"
```

## 2.5 Extra notes

For AES Counter mode (AES-CTR), the library supports two different sizes for Initialization Vector (IV):

- 12 bytes: used mainly for IPSec, as it requires 12 bytes from the user, which internally are appended the counter block (4 bytes), which is set to 1 for the first block (no padding required from the user)
- 16 bytes: when passing 16 bytes, the library will take them and use the last 4 bytes as the initial counter block for the first block.

## AES-NI GCM CRYPTO POLL MODE DRIVER

The AES-NI GCM PMD (`librte_pmd_aesni_gcm`) provides poll mode crypto driver support for utilizing Intel multi buffer library (see AES-NI Multi-buffer PMD documentation to learn more about it, including installation).

### 3.1 Features

AESNI GCM PMD has support for:

Authentication algorithms:

- `RTE_CRYPTOPATH_AES_GMAC`

AEAD algorithms:

- `RTE_CRYPTOPATH_AES_GCM`

### 3.2 Limitations

- Chained mbufs are supported but only out-of-place (destination mbuf must be contiguous).
- Cipher only is not supported.

### 3.3 Installation

To build DPDK with the `AESNI_GCM_PMD` the user is required to download the multi-buffer library from [here](https://github.com/01org/intel-ipsec-mb/archive/v0.50.zip) and compile it on their user system before building DPDK. The latest version of the library supported by this PMD is v0.50, which can be downloaded in <https://github.com/01org/intel-ipsec-mb/archive/v0.50.zip>.

```
make
make install
```

As a reference, the following table shows a mapping between the past DPDK versions and the external crypto libraries supported by them:



Table 3.1: DPDK and external crypto library version compatibility

DPDK version	Crypto library version
16.04 - 16.11	Multi-buffer library 0.43 - 0.44
17.02 - 17.05	ISA-L Crypto v2.18
17.08 - 18.02	Multi-buffer library 0.46 - 0.48
18.05+	Multi-buffer library 0.49+

### 3.4 Initialization

In order to enable this virtual crypto PMD, user must:

- Build the multi buffer library (explained in Installation section).
- Set `CONFIG_RTE_LIBRTE_PMD_AESNI_GCM=y` in `config/common_base`.

To use the PMD in an application, user must:

- Call `rte_vdev_init("crypto_aesni_gcm")` within the application.
- Use `-vdev="crypto_aesni_gcm"` in the EAL options, which will call `rte_vdev_init()` internally.

The following parameters (all optional) can be provided in the previous two calls:

- `socket_id`: Specify the socket where the memory for the device is going to be allocated (by default, `socket_id` will be the socket where the core that is creating the PMD is running on).
- `max_nb_queue_pairs`: Specify the maximum number of queue pairs in the device (8 by default).
- `max_nb_sessions`: Specify the maximum number of sessions that can be created (2048 by default).

Example:

```
./l2fwd-crypto -l 1 -n 4 --vdev="crypto_aesni_gcm,socket_id=0,max_nb_sessions=128" \
-- -p 1 --cdev SW --chain AEAD --aad_algo "aes-gcm"
```

## ARMV8 CRYPTO POLL MODE DRIVER

This code provides the initial implementation of the ARMv8 crypto PMD. The driver uses ARMv8 cryptographic extensions to process chained crypto operations in an optimized way. The core functionality is provided by a low-level library, written in the assembly code.

### 4.1 Features

ARMv8 Crypto PMD has support for the following algorithm pairs:

Supported cipher algorithms:

- RTE\_CRYPTO\_CIPHER\_AES\_CBC

Supported authentication algorithms:

- RTE\_CRYPTO\_AUTH\_SHA1\_HMAC
- RTE\_CRYPTO\_AUTH\_SHA256\_HMAC

### 4.2 Installation

In order to enable this virtual crypto PMD, user must:

- Download ARMv8 crypto library source code from [here](#)
- Export the environmental variable `ARMV8_CRYPTO_LIB_PATH` with the path where the `armv8_crypto` library was downloaded or cloned.
- Build the library by invoking:

```
make -C $ARMV8_CRYPTO_LIB_PATH/
```

- Set `CONFIG_RTE_LIBRTE_PMD_ARMV8_CRYPTO=y` in `config/defconfig_arm64-armv8a-linuxapp-gcc`

The corresponding device can be created only if the following features are supported by the CPU:

- RTE\_CPUFLAG\_AES
- RTE\_CPUFLAG\_SHA1
- RTE\_CPUFLAG\_SHA2
- RTE\_CPUFLAG\_NEON

## 4.3 Initialization

User can use app/test application to check how to use this PMD and to verify crypto processing.

Test name is cryptodev\_sw\_armv8\_autotest. For performance test cryptodev\_sw\_armv8\_perftest can be used.

## 4.4 Limitations

- Maximum number of sessions is 2048.
- Only chained operations are supported.
- AES-128-CBC is the only supported cipher variant.
- Cipher input data has to be a multiple of 16 bytes.
- Digest input data has to be a multiple of 8 bytes.

## AMD CCP POLL MODE DRIVER

This code provides the initial implementation of the ccp poll mode driver. The CCP poll mode driver library (librte\_pmd\_ccp) implements support for AMD's cryptographic co-processor (CCP). The CCP PMD is a virtual crypto poll mode driver which schedules crypto operations to one or more available CCP hardware engines on the platform. The CCP PMD provides poll mode crypto driver support for the following hardware accelerator devices:

```
AMD Cryptographic Co-processor (0x1456)
AMD Cryptographic Co-processor (0x1468)
```

### 5.1 Features

CCP crypto PMD has support for:

Cipher algorithms:

- RTE\_CRYPTO\_CIPHER\_AES\_CBC
- RTE\_CRYPTO\_CIPHER\_AES\_ECB
- RTE\_CRYPTO\_CIPHER\_AES\_CTR
- RTE\_CRYPTO\_CIPHER\_3DES\_CBC

Hash algorithms:

- RTE\_CRYPTO\_AUTH\_SHA1
- RTE\_CRYPTO\_AUTH\_SHA1\_HMAC
- RTE\_CRYPTO\_AUTH\_SHA224
- RTE\_CRYPTO\_AUTH\_SHA224\_HMAC
- RTE\_CRYPTO\_AUTH\_SHA256
- RTE\_CRYPTO\_AUTH\_SHA256\_HMAC
- RTE\_CRYPTO\_AUTH\_SHA384
- RTE\_CRYPTO\_AUTH\_SHA384\_HMAC
- RTE\_CRYPTO\_AUTH\_SHA512
- RTE\_CRYPTO\_AUTH\_SHA512\_HMAC
- RTE\_CRYPTO\_AUTH\_MD5\_HMAC
- RTE\_CRYPTO\_AUTH\_AES\_CMAC

- RTE\_CRYPTOP\_AUTH\_SHA3\_224
- RTE\_CRYPTOP\_AUTH\_SHA3\_224\_HMAC
- RTE\_CRYPTOP\_AUTH\_SHA3\_256
- RTE\_CRYPTOP\_AUTH\_SHA3\_256\_HMAC
- RTE\_CRYPTOP\_AUTH\_SHA3\_384
- RTE\_CRYPTOP\_AUTH\_SHA3\_384\_HMAC
- RTE\_CRYPTOP\_AUTH\_SHA3\_512
- RTE\_CRYPTOP\_AUTH\_SHA3\_512\_HMAC

AEAD algorithms:

- RTE\_CRYPTOP\_AEAD\_AES\_GCM

## 5.2 Installation

To compile ccp PMD, it has to be enabled in the config/common\_base file and openssl packages have to be installed in the build environment.

- CONFIG\_RTE\_LIBRTE\_PMD\_CCP=y

For Ubuntu 16.04 LTS use below to install openssl in the build system:

```
sudo apt-get install openssl
```

This code was verified on Ubuntu 16.04.

## 5.3 Initialization

Bind the CCP devices to DPDK UIO driver module before running the CCP PMD stack. e.g. for the 0x1456 device:

```
cd to the top-level DPDK directory
modprobe uio
insmod ./build/kmod/igb_uio.ko
echo "1022 1456" > /sys/bus/pci/drivers/igb_uio/new_id
```

Another way to bind the CCP devices to DPDK UIO driver is by using the dpdk-devbind.py script. The following command assumes BFD as 0000:09:00.2:

```
cd to the top-level DPDK directory
./usertools/dpdk-devbind.py -b igb_uio 0000:09:00.2
```

In order to enable the ccp crypto PMD, user must set CONFIG\_RTE\_LIBRTE\_PMD\_CCP=y in config/common\_base.

To use the PMD in an application, user must:

- Call rte\_vdev\_init("crypto\_ccp") within the application.
- Use -vdev="crypto\_ccp" in the EAL options, which will call rte\_vdev\_init() internally.

The following parameters (all optional) can be provided in the previous two calls:

- To validate ccp pmd, l2fwd-crypto example can be used with following command:

```
sudo ./build/l2fwd-crypto -l 1 -n 4 --vdev "crypto_ccp" -- -p 0x1  
--chain CIPHER_HASH --cipher_op ENCRYPT --cipher_algo AES_CBC  
--cipher_key 00:01:02:03:04:05:06:07:08:09:0a:0b:0c:0d:0e:0f  
--iv 00:01:02:03:04:05:06:07:08:09:0a:0b:0c:0d:0e:ff  
--auth_op GENERATE --auth_algo SHA1_HMAC  
--auth_key 11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:  
11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:  
.11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11
```

```
sudo ./build/l2fwd-crypto -l 1 -n 4 --vdev "crypto_ccp,ccp_auth_opt=1" -- -p 0x1  
--chain CIPHER_HASH --cipher_op ENCRYPT --cipher_algo AES_CBC  
--cipher_key 00:01:02:03:04:05:06:07:08:09:0a:0b:0c:0d:0e:0f  
--iv 00:01:02:03:04:05:06:07:08:09:0a:0b:0c:0d:0e:ff  
--auth_op GENERATE --auth_algo SHA1_HMAC  
--auth_key 11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:  
.11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:  
.11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:
```

- Chained mbufs are not supported.
- MD5 HMAC is supported only for CPU based authentication.

## NXP DPAA2 CAAM (DPAA2\_SEC)

The DPAA2\_SEC PMD provides poll mode crypto driver support for NXP DPAA2 CAAM hardware accelerator.

### 6.1 Architecture

SEC is the SOC's security engine, which serves as NXP's latest cryptographic acceleration and offloading hardware. It combines functions previously implemented in separate modules to create a modular and scalable acceleration and assurance engine. It also implements block encryption algorithms, stream cipher algorithms, hashing algorithms, public key algorithms, run-time integrity checking, and a hardware random number generator. SEC performs higher-level cryptographic operations than previous NXP cryptographic accelerators. This provides significant improvement to system level performance.

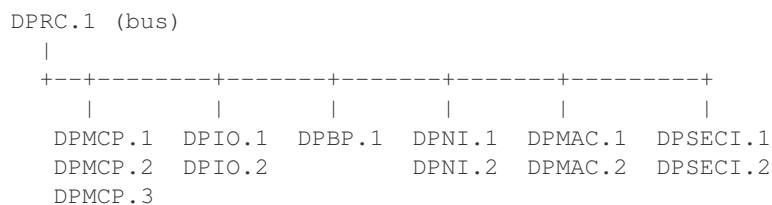
DPAA2\_SEC is one of the hardware resource in DPAA2 Architecture. More information on DPAA2 Architecture is described in `dpaa2_overview`.

DPAA2\_SEC PMD is one of DPAA2 drivers which interacts with Management Complex (MC) portal to access the hardware object - DPSECI. The MC provides access to create, discover, connect, configure and destroy `dpseci` objects in DPAA2\_SEC PMD.

DPAA2\_SEC PMD also uses some of the other hardware resources like buffer pools, queues, queue portals to store and to enqueue/dequeue data to the hardware SEC.

DPSECI objects are detected by PMD using a resource container called DPRC (like in `dpaa2_overview`).

For example:



### 6.2 Implementation

SEC provides platform assurance by working with SecMon, which is a companion logic block that tracks the security state of the SOC. SEC is programmed by means of descriptors (not to be confused with frame descriptors (FDs)) that indicate the operations to be performed and





- RTE\_CRYPTO\_AUTH\_SHA1\_HMAC
- RTE\_CRYPTO\_AUTH\_SHA224\_HMAC
- RTE\_CRYPTO\_AUTH\_SHA256\_HMAC
- RTE\_CRYPTO\_AUTH\_SHA384\_HMAC
- RTE\_CRYPTO\_AUTH\_SHA512\_HMAC
- RTE\_CRYPTO\_AUTH\_MD5\_HMAC

AEAD algorithms:

- RTE\_CRYPTO\_AEAD\_AES\_GCM

## 6.4 Supported DPAA2 SoCs

- LS2080A/LS2040A
- LS2084A/LS2044A
- LS2088A/LS2048A
- LS1088A/LS1048A

## 6.5 Whitelisting & Blacklisting

For blacklisting a DPAA2 SEC device, following commands can be used.

```
<dpdk app> <EAL args> -b "fslmc:dpseci.x" -- ...
```

Where x is the device object id as configured in resource container.

## 6.6 Limitations

- Hash followed by Cipher mode is not supported
- Only supports the session-oriented API implementation (session-less APIs are not supported).

## 6.7 Prerequisites

DPAA2\_SEC driver has similar pre-requisites as described in `dpaa2_overview`. The following dependencies are not part of DPDK and must be installed separately:

- **NXP Linux SDK**

NXP Linux software development kit (SDK) includes support for the family of QorIQ® ARM-Architecture-based system on chip (SoC) processors and corresponding boards.

It includes the Linux board support packages (BSPs) for NXP SoCs, a fully operational tool chain, kernel and board specific modules.

SDK and related information can be obtained from: [NXP QorIQ SDK](#).

- **DPDK Extra Scripts**

DPAA2 based resources can be configured easily with the help of ready scripts as provided in the DPDK helper repository.

[DPDK Extra Scripts](#).

Currently supported by DPDK:

- NXP SDK **17.08+**.
- MC Firmware version **10.3.1** and higher.
- Supported architectures: **arm64 LE**.
- Follow the DPDK Getting Started Guide for Linux to setup the basic DPDK environment.

## 6.8 Pre-Installation Configuration

### 6.8.1 Config File Options

Basic DPAA2 config file options are described in `dpaa2_overview`. In addition to those, the following options can be modified in the `config` file to enable DPAA2\_SEC PMD.

Please note that enabling debugging options may affect system performance.

- `CONFIG_RTE_LIBRTE_PMD_DPAA2_SEC` (default `n`) By default it is only enabled in `defconfig_arm64-dpaa2-*` config. Toggle compilation of the `librte_pmd_dpaa2_sec` driver.

## 6.9 Installations

To compile the DPAA2\_SEC PMD for Linux arm64 gcc target, run the following `make` command:

```
cd <DPDK-source-directory>
make config T=arm64-dpaa2-linuxapp-gcc install
```

### 6.10 Enabling logs

For enabling logs, use the following EAL parameter:

```
./your_crypto_application <EAL args> --log-level=pmd.crypto.dpaa2:<level>
```

Using `crypto.dpaa2` as log matching criteria, all Crypto PMD logs can be enabled which are lower than logging `level`.

## NXP DPAA CAAM (DPAA\_SEC)

The DPAA\_SEC PMD provides poll mode crypto driver support for NXP DPAA CAAM hardware accelerator.

### 7.1 Architecture

SEC is the SOC's security engine, which serves as NXP's latest cryptographic acceleration and offloading hardware. It combines functions previously implemented in separate modules to create a modular and scalable acceleration and assurance engine. It also implements block encryption algorithms, stream cipher algorithms, hashing algorithms, public key algorithms, run-time integrity checking, and a hardware random number generator. SEC performs higher-level cryptographic operations than previous NXP cryptographic accelerators. This provides significant improvement to system level performance.

DPAA\_SEC is one of the hardware resource in DPAA Architecture. More information on DPAA Architecture is described in `dpaa_overview`.

DPAA\_SEC PMD is one of DPAA drivers which interacts with QBMAN to create, configure and destroy the device instance using queue pair with CAAM portal.

DPAA\_SEC PMD also uses some of the other hardware resources like buffer pools, queues, queue portals to store and to enqueue/dequeue data to the hardware SEC.

### 7.2 Implementation

SEC provides platform assurance by working with SecMon, which is a companion logic block that tracks the security state of the SOC. SEC is programmed by means of descriptors (not to be confused with frame descriptors (FDs)) that indicate the operations to be performed and link to the message and associated data. SEC incorporates two DMA engines to fetch the descriptors, read the message data, and write the results of the operations. The DMA engine provides a scatter/gather capability so that SEC can read and write data scattered in memory. SEC may be configured by means of software for dynamic changes in byte ordering. The default configuration for this version of SEC is little-endian mode.

### 7.3 Features

The DPAA PMD has support for:

#### Cipher algorithms:

- RTE\_CRYPTOP\_CIPHER\_3DES\_CBC
- RTE\_CRYPTOP\_CIPHER\_AES128\_CBC
- RTE\_CRYPTOP\_CIPHER\_AES192\_CBC
- RTE\_CRYPTOP\_CIPHER\_AES256\_CBC
- RTE\_CRYPTOP\_CIPHER\_AES128\_CTR
- RTE\_CRYPTOP\_CIPHER\_AES192\_CTR
- RTE\_CRYPTOP\_CIPHER\_AES256\_CTR

#### Hash algorithms:

- RTE\_CRYPTOP\_AUTH\_SHA1\_HMAC
- RTE\_CRYPTOP\_AUTH\_SHA224\_HMAC
- RTE\_CRYPTOP\_AUTH\_SHA256\_HMAC
- RTE\_CRYPTOP\_AUTH\_SHA384\_HMAC
- RTE\_CRYPTOP\_AUTH\_SHA512\_HMAC
- RTE\_CRYPTOP\_AUTH\_MD5\_HMAC

#### AEAD algorithms:

- RTE\_CRYPTOP\_AEAD\_AES\_GCM

## 7.4 Supported DPAA SoCs

- LS1046A/LS1026A
- LS1043A/LS1023A

## 7.5 Whitelisting & Blacklisting

For blacklisting a DPAA device, following commands can be used.

```
<dpdk app> <EAL args> -b "dpaa_bus:dpaa-secX" -- ...  
e.g. "dpaa_bus:dpaa-sec0"
```

```
or to disable all 4 SEC devices
```

```
-b "dpaa_sec:dpaa-sec0" -b "dpaa_sec:dpaa-sec1" -b "dpaa_sec:dpaa-sec2" -b "dpaa_sec:dpaa-sec3"
```

## 7.6 Limitations

- Hash followed by Cipher mode is not supported
- Only supports the session-oriented API implementation (session-less APIs are not supported).

## 7.7 Prerequisites

DPAA\_SEC driver has similar pre-requisites as described in `dpaa_overview`. The following dependencies are not part of DPDK and must be installed separately:

- **NXP Linux SDK**

NXP Linux software development kit (SDK) includes support for the family of QorIQ® ARM-Architecture-based system on chip (SoC) processors and corresponding boards.

It includes the Linux board support packages (BSPs) for NXP SoCs, a fully operational tool chain, kernel and board specific modules.

SDK and related information can be obtained from: [NXP QorIQ SDK](#).

- **DPDK Extras Scripts**

DPAA based resources can be configured easily with the help of ready scripts as provided in the DPDK Extras repository.

[DPDK Extras Scripts](#).

Currently supported by DPDK:

- NXP SDK **2.0+**.
- Supported architectures: **arm64 LE**.
- Follow the DPDK Getting Started Guide for Linux to setup the basic DPDK environment.

## 7.8 Pre-Installation Configuration

### 7.8.1 Config File Options

Basic DPAA config file options are described in `dpaa_overview`. In addition to those, the following options can be modified in the `config` file to enable DPAA\_SEC PMD.

Please note that enabling debugging options may affect system performance.

- `CONFIG_RTE_LIBRTE_PMD_DPAA_SEC` (default `n`) By default it is only enabled in `defconfig_arm64-dpaa-*` config. Toggle compilation of the `librte_pmd_dpaa_sec` driver.

## 7.9 Installations

To compile the DPAA\_SEC PMD for Linux arm64 gcc target, run the following `make` command:

```
cd <DPDK-source-directory>
make config T=arm64-dpaa-linuxapp-gcc install
```

## 7.10 Enabling logs

For enabling logs, use the following EAL parameter:

```
./your_crypto_application <EAL args> --log-level=pmd.crypto.dpaa:<level>
```

Using `pmd.crypto.dpaa` as log matching criteria, all Crypto PMD logs can be enabled which are lower than logging `level`.

## KASUMI CRYPTO POLL MODE DRIVER

The KASUMI PMD (`librte_pmd_kasumi`) provides poll mode crypto driver support for utilizing Intel Libsso library, which implements F8 and F9 functions for KASUMI UEA1 cipher and UIA1 hash algorithms.

### 8.1 Features

KASUMI PMD has support for:

Cipher algorithm:

- `RTE_CRYPTOP_CIPHER_KASUMI_F8`

Authentication algorithm:

- `RTE_CRYPTOP_AUTH_KASUMI_F9`

### 8.2 Limitations

- Chained mbufs are not supported.
- KASUMI(F9) supported only if hash offset and length field is byte-aligned.
- In-place bit-level operations for KASUMI(F8) are not supported (if length and/or offset of data to be ciphered is not byte-aligned).

### 8.3 Installation

To build DPDK with the KASUMI\_PMD the user is required to download the export controlled `libsso_kasumi` library, by registering in [Intel Resource & Design Center](#). Once approval has been granted, the user needs to search for *Kasumi F8 F9 3GPP cryptographic algorithms Software Library* to download the library or directly through this [link](#). After downloading the library, the user needs to unpack and compile it on their system before building DPDK:

```
make
```

**Note:** When encrypting with KASUMI F8, by default the library encrypts full blocks of 8 bytes, regardless the number of bytes to be encrypted provided (which leads to a possible buffer overflow). To avoid this situation, it is necessary not to pass `3GPP_SAFE_BUFFERS` as a

compilation flag. Also, this is required when using chained operations (cipher-then-auth/auth-then-cipher). For this, in the Makefile of the library, make sure that this flag is commented out:

```
#EXTRA_CFLAGS += -D_3GPP_SAFE_BUFFERS
```

**Note:** To build the PMD as a shared library, the `libsso_kasumi` library must be built as follows:

```
make KASUMI_CFLAGS=-DKASUMI_C
```

## 8.4 Initialization

In order to enable this virtual crypto PMD, user must:

- Export the environmental variable `LIBSSO_KASUMI_PATH` with the path where the library was extracted (kasumi folder).
- Build the LIBSSO library (explained in Installation section).
- Set `CONFIG_RTE_LIBRTE_PMD_KASUMI=y` in `config/common_base`.

To use the PMD in an application, user must:

- Call `rte_vdev_init("crypto_kasumi")` within the application.
- Use `-vdev="crypto_kasumi"` in the EAL options, which will call `rte_vdev_init()` internally.

The following parameters (all optional) can be provided in the previous two calls:

- `socket_id`: Specify the socket where the memory for the device is going to be allocated (by default, `socket_id` will be the socket where the core that is creating the PMD is running on).
- `max_nb_queue_pairs`: Specify the maximum number of queue pairs in the device (8 by default).
- `max_nb_sessions`: Specify the maximum number of sessions that can be created (2048 by default).

Example:

```
./l2fwd-crypto -l 1 -n 4 --vdev="crypto_kasumi,socket_id=0,max_nb_sessions=128" \
-- -p 1 --cdev SW --chain CIPHER_ONLY --cipher_algo "kasumi-f8"
```

## 8.5 Extra notes on KASUMI F9

When using KASUMI F9 authentication algorithm, the input buffer must be constructed according to the 3GPP KASUMI specifications (section 4.4, page 13): <http://cryptome.org/3gpp/35201-900.pdf>. Input buffer has to have COUNT (4 bytes), FRESH (4 bytes), MESSAGE and DIRECTION (1 bit) concatenated. After the DIRECTION bit, a single '1' bit is appended, followed by between 0 and 7 '0' bits, so that the total length of the buffer is multiple of 8 bits. Note that the actual message can be any length, specified in bits.

Once this buffer is passed this way, when creating the crypto operation, length of data to authenticate (`op.sym.auth.data.length`) must be the length of all the items described above, including the padding at the end. Also, offset of data to authenticate (`op.sym.auth.data.offset`) must be such that points at the start of the COUNT bytes.



## OPENSSL CRYPTO POLL MODE DRIVER

This code provides the initial implementation of the openssl poll mode driver. All cryptography operations are using Openssl library crypto API. Each algorithm uses EVP interface from openssl API - which is recommended by Openssl maintainers.

For more details about openssl library please visit openssl webpage: <https://www.openssl.org/>

### 9.1 Features

OpenSSL PMD has support for:

Supported cipher algorithms:

- RTE\_CRYPTOP\_CIPHER\_3DES\_CBC
- RTE\_CRYPTOP\_CIPHER\_AES\_CBC
- RTE\_CRYPTOP\_CIPHER\_AES\_CTR
- RTE\_CRYPTOP\_CIPHER\_3DES\_CTR
- RTE\_CRYPTOP\_CIPHER\_DES\_DOCSISBPI

Supported authentication algorithms:

- RTE\_CRYPTOP\_AUTH\_AES\_GMAC
- RTE\_CRYPTOP\_AUTH\_MD5
- RTE\_CRYPTOP\_AUTH\_SHA1
- RTE\_CRYPTOP\_AUTH\_SHA224
- RTE\_CRYPTOP\_AUTH\_SHA256
- RTE\_CRYPTOP\_AUTH\_SHA384
- RTE\_CRYPTOP\_AUTH\_SHA512
- RTE\_CRYPTOP\_AUTH\_MD5\_HMAC
- RTE\_CRYPTOP\_AUTH\_SHA1\_HMAC
- RTE\_CRYPTOP\_AUTH\_SHA224\_HMAC
- RTE\_CRYPTOP\_AUTH\_SHA256\_HMAC
- RTE\_CRYPTOP\_AUTH\_SHA384\_HMAC

- RTE\_CRYPT0\_AUTH\_SHA512\_HMAC

Supported AEAD algorithms:

- RTE\_CRYPT0\_AEAD\_AES\_GCM
- RTE\_CRYPT0\_AEAD\_AES\_CCM

## 9.2 Installation

To compile openssl PMD, it has to be enabled in the config/common\_base file and appropriate openssl packages have to be installed in the build environment.

The newest openssl library version is supported:

- 1.0.2h-fips 3 May 2016.

Older versions that were also verified:

- 1.0.1f 6 Jan 2014
- 1.0.1 14 Mar 2012

For Ubuntu 14.04 LTS these packages have to be installed in the build system:

```
sudo apt-get install openssl
sudo apt-get install libc6-dev-i386 # for i686-native-linuxapp-gcc target
```

This code was also verified on Fedora 24. This code has NOT been verified on FreeBSD yet.

### 9.3 Initialization

User can use app/test application to check how to use this pmd and to verify crypto processing.

Test name is `cryptodev_openssl_autotest`. For performance test `cryptodev_openssl_perftest` can be used. For asymmetric crypto operations testing, run `cryptodev_openssl_asym_autotest`.

To verify real traffic `l2fwd-crypto` example can be used with this command:

```
sudo ./build/l2fwd-crypto -l 0-1 -n 4 --vdev "crypto_openssl"  
--vdev "crypto_openssl"-- -p 0x3 --chain CIPHER_HASH  
--cipher_op ENCRYPT --cipher_algo AES_CBC  
--cipher_key 00:01:02:03:04:05:06:07:08:09:0a:0b:0c:0d:0e:0f  
--iv 00:01:02:03:04:05:06:07:08:09:0a:0b:0c:0d:0e:ff  
--auth_op GENERATE --auth_algo SHA1_HMAC  
--auth_key 11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:  
11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:  
11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11
```

## 9.4 Limitations

- Maximum number of sessions is 2048.
- Chained mbufs are supported only for source mbuf (destination must be contiguous).
- Hash only is not supported for GCM and GMAC.

- Cipher only is not supported for GCM and GMAC.

## MVSAM CRYPTO POLL MODE DRIVER

The MVSAM CRYPTO PMD (`librte_crypto_mvsam_pmd`) provides poll mode crypto driver support by utilizing MUSDK library, which provides cryptographic operations acceleration by using Security Acceleration Engine (EIP197) directly from user-space with minimum overhead and high performance.

### 10.1 Features

MVSAM CRYPTO PMD has support for:

- Symmetric crypto
- Sym operation chaining
- AES CBC (128)
- AES CBC (192)
- AES CBC (256)
- AES CTR (128)
- AES CTR (192)
- AES CTR (256)
- 3DES CBC
- 3DES CTR
- MD5
- MD5 HMAC
- SHA1
- SHA1 HMAC
- SHA256
- SHA256 HMAC
- SHA384
- SHA384 HMAC
- SHA512
- SHA512 HMAC

- AES GCM (128)

## 10.2 Limitations

- Hardware only supports scenarios where ICV (digest buffer) is placed just after the authenticated data. Other placement will result in error.

## 10.3 Installation

MVSAM CRYPTO PMD driver compilation is disabled by default due to external dependencies. Currently there are two driver specific compilation options in `config/common_base` available:

- `CONFIG_RTE_LIBRTE_MVSAM_CRYPTO` (default `n`)  
Toggle compilation of the `librte_pmd_mvsam` driver.
- `CONFIG_RTE_LIBRTE_MVSAM_CRYPTO_DEBUG` (default `n`)  
Toggle display of debugging messages.

For a list of prerequisites please refer to *Prerequisites* section in MVPP2 Poll Mode Driver guide.

MVSAM CRYPTO PMD requires MUSDK built with EIP197 support thus following extra option must be passed to the library configuration script:

```
--enable-sam
```

For `crypto_safexcel.ko` module build instructions please refer to `doc/musdk_get_started.txt`.

## 10.4 Initialization

After successfully building MVSAM CRYPTO PMD, the following modules need to be loaded:

```
insmod musdk_uio.ko
insmod mvpp2x_sysfs.ko
insmod mv_pp_uio.ko
insmod mv_sam_uio.ko
insmod crypto_safexcel.ko
```

The following parameters (all optional) are exported by the driver:

- `max_nb_queue_pairs`: maximum number of queue pairs in the device (8 by default).
- `max_nb_sessions`: maximum number of sessions that can be created (2048 by default).
- `socket_id`: socket on which to allocate the device resources on.

`l2fwd-crypto` example application can be used to verify MVSAM CRYPTO PMD operation:

```
./l2fwd-crypto --vdev=eth_mvpp2,iface=eth0 --vdev=crypto_mvsam -- \
--cipher_op ENCRYPT --cipher_algo aes-cbc \
--cipher_key 00:01:02:03:04:05:06:07:08:09:0a:0b:0c:0d:0e:0f \
--auth_op GENERATE --auth_algo sha1-hmac \
--auth_key 10:11:12:13:14:15:16:17:18:19:1a:1b:1c:1d:1e:1f
```

Example output:

```

[...]
```

AAD: at [0x7f253ceb80], len=  
P ID 0 configuration ----  
Port mode : KR  
MAC status : disabled  
Link status : link up  
Port speed : 10G  
Port duplex : full  
Port: Egress enable tx\_port\_num=16 qmap=0x1  
PORT: Port0 - link  
P ID 0 configuration ----  
Port mode : KR  
MAC status : disabled  
Link status : link down  
Port speed : 10G  
Port duplex : full  
Port: Egress enable tx\_port\_num=16 qmap=0x1  
Port 0, MAC address: 00:50:43:02:21:20

Checking link statusdone  
Port 0 Link Up - speed 0 Mbps - full-duplex  
Lcore 0: RX port 0  
Allocated session pool on socket 0  
eip197: 0:0 registers: paddr: 0xf2880000, vaddr: 0x0x7f56a80000  
DMA buffer (131136 bytes) for CDR #0 allocated: paddr = 0xb0585e00, vaddr = 0x7f09384e00  
DMA buffer (131136 bytes) for RDR #0 allocated: paddr = 0xb05a5f00, vaddr = 0x7f093a4f00  
DMA buffers allocated for 2049 operations. Tokens - 256 bytes  
Lcore 0: cryptodev 0  
L2FWD: lcore 1 has nothing to do  
L2FWD: lcore 2 has nothing to do  
L2FWD: lcore 3 has nothing to do  
L2FWD: entering main loop on lcore 0  
L2FWD: -- lcoreid=0 portid=0  
L2FWD: -- lcoreid=0 cryptoid=0  
Options:-  
nportmask: ffffffff  
ports per lcore: 1  
refresh period : 10000  
single lcore mode: disabled  
stats\_printing: enabled  
sessionless crypto: disabled

Crypto chain: Input --> Encrypt --> Auth generate --> Output

---- Cipher information ---  
Algorithm: aes-cbc  
Cipher key: at [0x7f56db4e80], len=16  
00000000: 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F | .....  
IV: at [0x7f56db4b80], len=16  
00000000: 20 F0 63 0E 45 EB 2D 84 72 D4 13 6E 36 B5 AF FE | .c.E.-.r..n6...

---- Authentication information ---  
Algorithm: sha1-hmac  
Auth key: at [0x7f56db4d80], len=16  
00000000: 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F | .....  
IV: at [0x7f56db4a80], len=0  
AAD: at [0x7f253ceb80], len=

## NULL CRYPTO POLL MODE DRIVER

The Null Crypto PMD (**librte\_pmd\_null\_crypto**) provides a crypto poll mode driver which provides a minimal implementation for a software crypto device. As a null device it does not modify the data in the mbuf on which the crypto operation is to operate and it only has support for a single cipher and authentication algorithm.

When a burst of mbufs is submitted to a Null Crypto PMD for processing then each mbuf in the burst will be enqueued in an internal buffer for collection on a dequeue call as long as the mbuf has a valid `rte_mbuf_offload` operation with a valid `rte_cryptodev_session` or `rte_crypto_xform` chain of operations.

### 11.1 Features

Modes:

- `RTE_CRYPTOTO_XFORM_CIPHER ONLY`
- `RTE_CRYPTOTO_XFORM_AUTH ONLY`
- `RTE_CRYPTOTO_XFORM_CIPHER THEN RTE_CRYPTOTO_XFORM_AUTH`
- `RTE_CRYPTOTO_XFORM_AUTH THEN RTE_CRYPTOTO_XFORM_CIPHER`

Cipher algorithms:

- `RTE_CRYPTOTO_CIPHER_NULL`

Authentication algorithms:

- `RTE_CRYPTOTO_AUTH_NULL`

### 11.2 Limitations

- Only in-place is currently supported (destination address is the same as source address).

### 11.3 Installation

The Null Crypto PMD is enabled and built by default in both the Linux and FreeBSD builds.

## 11.4 Initialization

To use the PMD in an application, user must:

- Call `rte_vdev_init("crypto_null")` within the application.
- Use `-vdev="crypto_null"` in the EAL options, which will call `rte_vdev_init()` internally.

The following parameters (all optional) can be provided in the previous two calls:

- `socket_id`: Specify the socket where the memory for the device is going to be allocated (by default, `socket_id` will be the socket where the core that is creating the PMD is running on).
- `max_nb_queue_pairs`: Specify the maximum number of queue pairs in the device (8 by default).
- `max_nb_sessions`: Specify the maximum number of sessions that can be created (2048 by default).

Example:

```
./l2fwd-crypto -l 1 -n 4 --vdev="crypto_null,socket_id=0,max_nb_sessions=128" \  
-- -p 1 --cdev SW --chain CIPHER_ONLY --cipher_algo "null"
```



## CRYPTODEV SCHEDULER POLL MODE DRIVER LIBRARY

Scheduler PMD is a software crypto PMD, which has the capabilities of attaching hardware and/or software cryptodevs, and distributes ingress crypto ops among them in a certain manner.

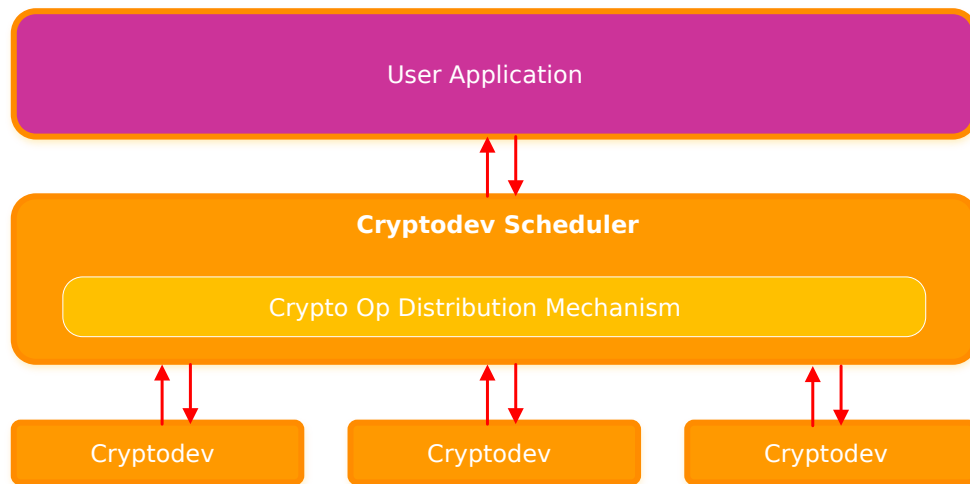


Fig. 12.1: Cryptodev Scheduler Overview

The Cryptodev Scheduler PMD library (**librte\_pmd\_crypto\_scheduler**) acts as a software crypto PMD and shares the same API provided by **librte\_cryptodev**. The PMD supports attaching multiple crypto PMDs, software or hardware, as slaves, and distributes the crypto workload to them with certain behavior. The behaviors are categorized as different “modes”. Basically, a scheduling mode defines certain actions for scheduling crypto ops to its slaves.

The **librte\_pmd\_crypto\_scheduler** library exports a C API which provides an API for attaching/detaching slaves, set/get scheduling modes, and enable/disable crypto ops reordering.

### 12.1 Limitations

- Sessionless crypto operation is not supported
- OOP crypto operation is not supported when the crypto op reordering feature is enabled.

## 12.2 Installation

To build DPDK with CRYPTPO\_SCHEDULER\_PMD the user is required to set CONFIG\_RTE\_LIBRTE\_PMD\_CRYPTPO\_SCHEDULER=y in config/common\_base, and recompile DPDK

## 12.3 Initialization

To use the PMD in an application, user must:

- Call `rte_vdev_init("crypto_scheduler")` within the application.
- Use `--vdev="crypto_scheduler"` in the EAL options, which will call `rte_vdev_init()` internally.

The following parameters (all optional) can be provided in the previous two calls:

- `socket_id`: Specify the socket where the memory for the device is going to be allocated (by default, `socket_id` will be the socket where the core that is creating the PMD is running on).
- `max_nb_sessions`: Specify the maximum number of sessions that can be created. This value may be overwritten internally if there are too many devices are attached.
- `slave`: If a cryptodev has been initialized with specific name, it can be attached to the scheduler using this parameter, simply filling the name here. Multiple cryptodevs can be attached initially by presenting this parameter multiple times.
- `mode`: Specify the scheduling mode of the PMD. The supported scheduling mode parameter values are specified in the "Cryptodev Scheduler Modes Overview" section.
- `mode_param`: Specify the mode-specific parameter. Some scheduling modes may be initialized with specific parameters other than the default ones, such as the **threshold** packet size of **packet-size-distr** mode. This parameter fulfills the purpose.
- `ordering`: Specify the status of the crypto operations ordering feature. The value of this parameter can be "enable" or "disable". This feature is disabled by default.

Example:

```
... --vdev "crypto_aesni_mb0,name=aesni_mb_1" --vdev "crypto_aesni_mb1,name=aesni_mb_2" --vdev
```

---

### Note:

- The scheduler cryptodev cannot be started unless the scheduling mode is set and at least one slave is attached. Also, to configure the scheduler in the run-time, like attach/detach slave(s), change scheduling mode, or enable/disable crypto op ordering, one should stop the scheduler first, otherwise an error will be returned.
  - The crypto op reordering feature requires using the userdata field of every mbuf to be processed to store temporary data. By the end of processing, the field is set to pointing to NULL, any previously stored value of this field will be lost.
-

## 12.4 Cryptodev Scheduler Modes Overview

Currently the Crypto Scheduler PMD library supports following modes of operation:

- **CDEV\_SCHED\_MODE\_ROUNDROBIN:**

*Initialization mode parameter:* **round-robin**

Round-robin mode, which distributes the enqueued burst of crypto ops among its slaves in a round-robin manner. This mode may help to fill the throughput gap between the physical core and the existing cryptodevs to increase the overall performance.

- **CDEV\_SCHED\_MODE\_PKT\_SIZE\_DISTR:**

*Initialization mode parameter:* **packet-size-distr**

Packet-size based distribution mode, which works with 2 slaves, the primary slave and the secondary slave, and distributes the enqueued crypto operations to them based on their data lengths. A crypto operation will be distributed to the primary slave if its data length is equal to or bigger than the designated threshold, otherwise it will be handled by the secondary slave.

A typical usecase in this mode is with the QAT cryptodev as the primary and a software cryptodev as the secondary slave. This may help applications to process additional crypto workload than what the QAT cryptodev can handle on its own, by making use of the available CPU cycles to deal with smaller crypto workloads.

The threshold is set to 128 bytes by default. It can be updated by calling function **rte\_cryptodev\_scheduler\_option\_set**. The parameter of **option\_type** must be **CDEV\_SCHED\_OPTION\_THRESHOLD** and **option** should point to a **rte\_cryptodev\_scheduler\_threshold\_option** structure filled with appropriate threshold value. Please NOTE this threshold has to be a power-of-2 unsigned integer. It is possible to use **mode\_param** initialization parameter to achieve the same purpose. For example:

```
... -vddev "crypto_scheduler,mode=packet-size-distr,mode_param=threshold:512"
...
```

The above parameter will overwrite the threshold value to 512.

- **CDEV\_SCHED\_MODE\_FAILOVER:**

*Initialization mode parameter:* **fail-over**

Fail-over mode, which works with 2 slaves, the primary slave and the secondary slave. In this mode, the scheduler will enqueue the incoming crypto operation burst to the primary slave. When one or more crypto operations fail to be enqueued, then they will be enqueued to the secondary slave.

- **CDEV\_SCHED\_MODE\_MULTICORE:**

*Initialization mode parameter:* **multi-core**

Multi-core mode, which distributes the workload with several (up to eight) worker cores. The enqueued bursts are distributed among the worker cores in a round-robin manner. If scheduler cannot enqueue entire burst to the same worker, it will enqueue the remaining operations to the next available worker. For pure small packet size (64 bytes) traffic however the multi-core mode is not an optimal solution,

as it doesn't give significant per-core performance improvement. For mixed traffic (IMIX) the optimal number of worker cores is around 2-3. For large packets (1.5 Kbytes) scheduler shows linear scaling in performance up to eight cores. Each worker uses its own slave cryptodev. Only software cryptodevs are supported. Only the same type of cryptodevs should be used concurrently.

The multi-core mode uses one extra parameter:

- **corelist**: Semicolon-separated list of logical cores to be used as workers. The number of worker cores should be equal to the number of slave cryptodevs. These cores should be present in EAL core list parameter and should not be used by the application or any other process.

**Example:** ...                    -vdev        "crypto\_aesni\_mb1,name=aesni\_mb\_1"        -  
vdev                    "crypto\_aesni\_mb\_pmd2,name=aesni\_mb\_2"                    -vdev  
"crypto\_scheduler,slave=aesni\_mb\_1,slave=aesni\_mb\_2,mode=multi-  
core,corelist=23;24" ...

## SNOW 3G CRYPTO POLL MODE DRIVER

The SNOW 3G PMD (`librte_pmd_snow3g`) provides poll mode crypto driver support for utilizing Intel Libsso library, which implements F8 and F9 functions for SNOW 3G UEA2 cipher and UIA2 hash algorithms.

### 13.1 Features

SNOW 3G PMD has support for:

Cipher algorithm:

- `RTE_CRYPTOP_CIPHER_SNOW3G_UEA2`

Authentication algorithm:

- `RTE_CRYPTOP_AUTH_SNOW3G_UIA2`

### 13.2 Limitations

- Chained mbufs are not supported.
- SNOW 3G (UIA2) supported only if hash offset field is byte-aligned.
- In-place bit-level operations for SNOW 3G (UEA2) are not supported (if length and/or offset of data to be ciphered is not byte-aligned).

### 13.3 Installation

To build DPDK with the SNOW3G\_PMD the user is required to download the export controlled `libsso_snow3g` library, by registering in [Intel Resource & Design Center](#). Once approval has been granted, the user needs to search for *Snow3G F8 F9 3GPP cryptographic algorithms Software Library* to download the library or directly through this [link](#). After downloading the library, the user needs to unpack and compile it on their system before building DPDK:

```
make snow3g
```

**Note:** When encrypting with SNOW3G UEA2, by default the library encrypts blocks of 4 bytes, regardless the number of bytes to be encrypted provided (which leads to a possible buffer overflow). To avoid this situation, it is necessary not to pass `3GPP_SAFE_BUFFERS` as a compilation flag. For this, in the Makefile of the library, make sure that this flag is commented out.:

```
#EXTRA_CFLAGS += -D_3GPP_SAFE_BUFFERS
```

## 13.4 Initialization

In order to enable this virtual crypto PMD, user must:

- Export the environmental variable LIBSSO\_SNOW3G\_PATH with the path where the library was extracted (snow3g folder).
- Build the LIBSSO\_SNOW3G library (explained in Installation section).
- Set CONFIG\_RTE\_LIBRTE\_PMD\_SNOW3G=y in config/common\_base.

To use the PMD in an application, user must:

- Call `rte_vdev_init("crypto_snow3g")` within the application.
- Use `-vdev="crypto_snow3g"` in the EAL options, which will call `rte_vdev_init()` internally.

The following parameters (all optional) can be provided in the previous two calls:

- `socket_id`: Specify the socket where the memory for the device is going to be allocated (by default, `socket_id` will be the socket where the core that is creating the PMD is running on).
- `max_nb_queue_pairs`: Specify the maximum number of queue pairs in the device (8 by default).
- `max_nb_sessions`: Specify the maximum number of sessions that can be created (2048 by default).

Example:

```
./l2fwd-crypto -l 1 -n 4 --vdev="crypto_snow3g,socket_id=0,max_nb_sessions=128" \  
-- -p 1 --cdev SW --chain CIPHER_ONLY --cipher_algo "snow3g-uea2"
```

## **INTEL(R) QUICKASSIST (QAT) CRYPTO POLL MODE DRIVER**

The QAT PMD provides poll mode crypto driver support for the following hardware accelerator devices:

- Intel QuickAssist Technology DH895xCC
- Intel QuickAssist Technology C62x
- Intel QuickAssist Technology C3xxx
- Intel QuickAssist Technology D15xx

### **14.1 Features**

The QAT PMD has support for:

Cipher algorithms:

- RTE\_CRYPTO\_CIPHER\_3DES\_CBC
- RTE\_CRYPTO\_CIPHER\_3DES\_CTR
- RTE\_CRYPTO\_CIPHER\_AES128\_CBC
- RTE\_CRYPTO\_CIPHER\_AES192\_CBC
- RTE\_CRYPTO\_CIPHER\_AES256\_CBC
- RTE\_CRYPTO\_CIPHER\_AES128\_CTR
- RTE\_CRYPTO\_CIPHER\_AES192\_CTR
- RTE\_CRYPTO\_CIPHER\_AES256\_CTR
- RTE\_CRYPTO\_CIPHER\_SNOW3G\_UEA2
- RTE\_CRYPTO\_CIPHER\_NULL
- RTE\_CRYPTO\_CIPHER\_KASUMI\_F8
- RTE\_CRYPTO\_CIPHER\_DES\_CBC
- RTE\_CRYPTO\_CIPHER\_AES\_DOCSISBPI
- RTE\_CRYPTO\_CIPHER\_DES\_DOCSISBPI
- RTE\_CRYPTO\_CIPHER\_ZUC\_EEA3

Hash algorithms:

- RTE\_CRYPT0\_AUTH\_SHA1\_HMAC
- RTE\_CRYPT0\_AUTH\_SHA224\_HMAC
- RTE\_CRYPT0\_AUTH\_SHA256\_HMAC
- RTE\_CRYPT0\_AUTH\_SHA384\_HMAC
- RTE\_CRYPT0\_AUTH\_SHA512\_HMAC
- RTE\_CRYPT0\_AUTH\_AES\_XCBC\_MAC
- RTE\_CRYPT0\_AUTH\_SNOW3G\_UIA2
- RTE\_CRYPT0\_AUTH\_MD5\_HMAC
- RTE\_CRYPT0\_AUTH\_NULL
- RTE\_CRYPT0\_AUTH\_KASUMI\_F9
- RTE\_CRYPT0\_AUTH\_AES\_GMAC
- RTE\_CRYPT0\_AUTH\_ZUC\_EIA3

Supported AEAD algorithms:

- RTE\_CRYPT0\_AEAD\_AES\_GCM

## 14.2 Limitations

- Only supports the session-oriented API implementation (session-less APIs are not supported).
- SNOW 3G (UEA2), KASUMI (F8) and ZUC (EEA3) supported only if cipher length and offset fields are byte-multiple.
- SNOW 3G (UIA2) and ZUC (EIA3) supported only if hash length and offset fields are byte-multiple.
- No BSD support as BSD QAT kernel driver not available.
- ZUC EEA3/EIA3 is not supported by dh895xcc devices
- Maximum additional authenticated data (AAD) for GCM is 240 bytes long.
- Queue pairs are not thread-safe (that is, within a single queue pair, RX and TX from different lcores is not supported).

## 14.3 Extra notes on KASUMI F9

When using KASUMI F9 authentication algorithm, the input buffer must be constructed according to the 3GPP KASUMI specifications (section 4.4, page 13): <http://cryptome.org/3gpp/35201-900.pdf>. Input buffer has to have COUNT (4 bytes), FRESH (4 bytes), MESSAGE and DIRECTION (1 bit) concatenated. After the DIRECTION bit, a single '1' bit is appended, followed by between 0 and 7 '0' bits, so that the total length of the buffer is multiple of 8 bits. Note that the actual message can be any length, specified in bits.

Once this buffer is passed this way, when creating the crypto operation, length of data to authenticate (op.sym.auth.data.length) must be the length of all the items described above,



including the padding at the end. Also, offset of data to authenticate (op.sym.auth.data.offset) must be such that points at the start of the COUNT bytes.

## 14.4 Building the DPDK QAT cryptodev PMD

To enable QAT crypto in DPDK, follow the instructions for modifying the compile-time configuration file as described [here](#).

Quick instructions are as follows:

```
cd to the top-level DPDK directory
make config T=x86_64-native-linuxapp-gcc
sed -i 's,\(CONFIG_RTE_LIBRTE_PMD_QAT\) =n,\1=y,' build/.config
sed -i 's,\(CONFIG_RTE_LIBRTE_PMD_QAT_SYM\) =n,\1=y,' build/.config
make
```

## 14.5 Dependency on the QAT kernel driver

To use the QAT PMD an SRIOV-enabled QAT kernel driver is required. The VF devices created and initialised by this driver will be used by the QAT PMD.

Instructions for installation are below, but first an explanation of the relationships between the PF/VF devices and the PMDs visible to DPDK applications.

Acceleration services - cryptography and compression - are provided to DPDK applications via PMDs which register to implement the corresponding cryptodev and compressdev APIs.

Each QuickAssist VF device can expose one cryptodev PMD and/or one compressdev PMD. These QAT PMDs share the same underlying device and pci-mgmt code, but are enumerated independently on their respective APIs and appear as independent devices to applications.

---

**Note:** Each VF can only be used by one DPDK process. It is not possible to share the same VF across multiple processes, even if these processes are using different acceleration services.

Conversely one DPDK process can use one or more QAT VFs and can expose both cryptodev and compressdev instances on each of those VFs.

---

## 14.6 Device and driver naming

- The qat cryptodev driver name is “crypto\_qat”. The `rte_cryptodev_devices_get()` returns the devices exposed by this driver.
- Each qat crypto device has a unique name, in format `<pci bdf>_<service>`, e.g. “0000:41:01.0\_qat\_sym”. This name can be passed to `rte_cryptodev_get_dev_id()` to get the `device_id`.

---

**Note:** The qat crypto driver name is passed to the `dpdk-test-crypto-perf` tool in the `-devtype` parameter.

The qat crypto device name is in the format of the slave parameter passed to the crypto scheduler.

- The qat compressdev driver name is “comp\_qat”. The `rte_compressdev_devices_get()` returns the devices exposed by this driver.
- Each qat compression device has a unique name, in format `<pci bdf>_<service>`, e.g. “0000:41:01.0\_qat\_comp”. This name can be passed to `rte_compressdev_get_dev_id()` to get the `device_id`.

## 14.7 Available kernel drivers

Kernel drivers for each device are listed in the following table. Scroll right to check that the driver and device supports the service you require.

Table 14.1: QAT device generations, devices and drivers

Gen	Device	Driver/version	Kernel Module	Pci Driver	PF Did	#PFs	VF Did	VFs/PF	Cryptodev	compress-dev
1	DH895xx	linux/4.4+ 01.org/4.2.0+	qat_dh895xx	dh895xx	435	1	443	32	Yes	No
“	“	01.org/4.2.0+	“	“	“	“	“	“	Yes	No
2	C62x	linux/4.5+ 01.org/4.2.0+	qat_c62x	c6xx	37c8	3	37c9	16	Yes	No
“	“	01.org/4.2.0+	“	“	“	“	“	“	Yes	Yes
2	C3xxx	linux/4.5+ 01.org/4.2.0+	qat_c3xxx	c3xxx	19e2	1	19e3	16	Yes	No
“	“	01.org/4.2.0+	“	“	“	“	“	“	Yes	Yes
2	D15xx	p	qat_d15xx	d15xx	6f54	1	6f55	16	Yes	No

The `Driver` column indicates either the Linux kernel version in which support for this device was introduced or a driver available on Intel’s 01.org website. There are both linux and 01.org kernel drivers available for some devices. p = release pending.

If you are running on a kernel which includes a driver for your device, see [Installation using kernel.org driver](#) below. Otherwise see [Installation using 01.org QAT driver](#).

## 14.8 Installation using kernel.org driver

The examples below are based on the C62x device, if you have a different device use the corresponding values in the above table.

In BIOS ensure that SRIOV is enabled and either:

- Disable VT-d or
- Enable VT-d and set “`intel_iommu=on iommu=pt`” in the grub file.

Check that the QAT driver is loaded on your system, by executing:

```
lsmod | grep qa
```

You should see the kernel module for your device listed, e.g.:

```
qat_c62x          5626  0
intel_qat        82336  1 qat_c62x
```

Next, you need to expose the Virtual Functions (VFs) using the sysfs file system.

First find the BDFs (Bus-Device-Function) of the physical functions (PFs) of your device, e.g.:

```
lspci -d:37c8
```

You should see output similar to:

```
1a:00.0 Co-processor: Intel Corporation Device 37c8
3d:00.0 Co-processor: Intel Corporation Device 37c8
3f:00.0 Co-processor: Intel Corporation Device 37c8
```

Enable the VFs for each PF by echoing the number of VFs per PF to the pci driver:

```
echo 16 > /sys/bus/pci/drivers/c6xx/0000:1a:00.0/sriov_numvfs
echo 16 > /sys/bus/pci/drivers/c6xx/0000:3d:00.0/sriov_numvfs
echo 16 > /sys/bus/pci/drivers/c6xx/0000:3f:00.0/sriov_numvfs
```

Check that the VFs are available for use. For example `lspci -d:37c9` should list 48 VF devices available for a C62x device.

To complete the installation follow the instructions in [Binding the available VFs to the DPDK UIO driver](#).

---

**Note:** If the QAT kernel modules are not loaded and you see an error like `Failed to load MMP firmware qat_895xcc_mmp.bin` in kernel logs, this may be as a result of not using a distribution, but just updating the kernel directly.

Download firmware from the [kernel firmware repo](#).

Copy qat binaries to `/lib/firmware`:

```
cp qat_895xcc.bin /lib/firmware
cp qat_895xcc_mmp.bin /lib/firmware
```

Change to your linux source root directory and start the qat kernel modules:

```
insmod ./drivers/crypto/qat/qat_common/intel_qat.ko
insmod ./drivers/crypto/qat/qat_dh895xcc/qat_dh895xcc.ko
```

---

**Note:** If you see the following warning in `/var/log/messages` it can be ignored: `IOMMU should be enabled for SR-IOV to work correctly`.

---

## 14.9 Installation using 01.org QAT driver

Download the latest QuickAssist Technology Driver from [01.org](#). Consult the *Getting Started Guide* at the same URL for further information.

The steps below assume you are:

- Building on a platform with one C62x device.
- Using package `qat1.7.1.4.2.0-000xx.tar.gz`.
- On Fedora26 kernel `4.11.11-300.fc26.x86_64`.

In the BIOS ensure that SRIOV is enabled and VT-d is disabled.

Uninstall any existing QAT driver, for example by running:

- `./installer.sh uninstall` in the directory where originally installed.

Build and install the SRIOV-enabled QAT driver:

```
mkdir /QAT
cd /QAT

# Copy the package to this location and unpack
tar xzof qat1.7.1.4.2.0-000xx.tar.gz

./configure --enable-icp-sriov=host
make install
```

You can use `cat /sys/kernel/debug/qat<your device type and bdf>/version/fw` to confirm the driver is correctly installed and is using firmware version 4.2.0. You can use `lspci -d:37c9` to confirm the presence of the 16 VF devices available per C62x PF.

Confirm the driver is correctly installed and is using firmware version 4.2.0:

```
cat /sys/kernel/debug/qat<your device type and bdf>/version/fw
```

Confirm the presence of 48 VF devices - 16 per PF:

```
lspci -d:37c9
```

To complete the installation - follow instructions in [Binding the available VFs to the DPDK UIO driver](#).

---

**Note:** If using a later kernel and the build fails with an error relating to `strict_stroul` not being available apply the following patch:

```
/QAT/QAT1.6/quickassist/utilities/downloader/Target_CoreLibs/uclo/include/linux/uclo_platform.h
+ #if LINUX_VERSION_CODE >= KERNEL_VERSION(3,18,5)
+ #define STR_TO_64(str, base, num, endPtr) {endPtr=NULL; if (kstrtoul((str), (base), (num))) p
+ #else
+ #if LINUX_VERSION_CODE >= KERNEL_VERSION(2,6,38)
+ #define STR_TO_64(str, base, num, endPtr) {endPtr=NULL; if (strict_strtoul((str), (base), (num
+ #else
+ #if LINUX_VERSION_CODE >= KERNEL_VERSION(2,6,25)
+ #define STR_TO_64(str, base, num, endPtr) {endPtr=NULL; strict_strtoll((str), (base), (num));}
+ #else
+ #define STR_TO_64(str, base, num, endPtr)
+     do {
+         if (str[0] == '-')
+         {
+             *(num) = -(simple_strtoul((str+1), &(endPtr), (base)));
+         }else {
+             *(num) = simple_strtoul((str), &(endPtr), (base));
+         }
+     } while(0)
+ #endif
+ #endif
+ #endif
```

---

**Note:** If the build fails due to missing header files you may need to do following:

```
sudo yum install zlib-devel
sudo yum install openssl-devel
sudo yum install libudev-devel
```

---

**Note:** If the build or install fails due to mismatching kernel sources you may need to do the following:

```
sudo yum install kernel-headers-`uname -r`
sudo yum install kernel-src-`uname -r`
```

```
sudo yum install kernel-devel-`uname -r`
```

---

## 14.10 Binding the available VFs to the DPDK UIO driver

Unbind the VFs from the stock driver so they can be bound to the uio driver.

### 14.10.1 For an Intel(R) QuickAssist Technology DH895xCC device

The unbind command below assumes BDFs of 03:01.00–03:04.07, if your VFs are different adjust the unbind command below:

```
for device in $(seq 1 4); do \  
    for fn in $(seq 0 7); do \  
        echo -n 0000:03:0${device}.${fn} > \  
            /sys/bus/pci/devices/0000\:03\:0${device}.${fn}/driver/unbind; \  
    done; \  
done
```

### 14.10.2 For an Intel(R) QuickAssist Technology C62x device

The unbind command below assumes BDFs of 1a:01.00–1a:02.07, 3d:01.00–3d:02.07 and 3f:01.00–3f:02.07, if your VFs are different adjust the unbind command below:

```
for device in $(seq 1 2); do \  
    for fn in $(seq 0 7); do \  
        echo -n 0000:1a:0${device}.${fn} > \  
            /sys/bus/pci/devices/0000\:1a\:0${device}.${fn}/driver/unbind; \  
  
        echo -n 0000:3d:0${device}.${fn} > \  
            /sys/bus/pci/devices/0000\:3d\:0${device}.${fn}/driver/unbind; \  
  
        echo -n 0000:3f:0${device}.${fn} > \  
            /sys/bus/pci/devices/0000\:3f\:0${device}.${fn}/driver/unbind; \  
    done; \  
done
```

### 14.10.3 For Intel(R) QuickAssist Technology C3xxx or D15xx device

The unbind command below assumes BDFs of 01:01.00–01:02.07, if your VFs are different adjust the unbind command below:

```
for device in $(seq 1 2); do \  
    for fn in $(seq 0 7); do \  
        echo -n 0000:01:0${device}.${fn} > \  
            /sys/bus/pci/devices/0000\:01\:0${device}.${fn}/driver/unbind; \  
    done; \  
done
```

### 14.10.4 Bind to the DPDK uio driver

Install the DPDK igb\_uio driver, bind the VF PCI Device id to it and use lspci to confirm the VF devices are now in use by igb\_uio kernel driver, e.g. for the C62x device:

```
cd to the top-level DPDK directory
modprobe uio
insmod ./build/kmod/igb_uio.ko
echo "8086 37c9" > /sys/bus/pci/drivers/igb_uio/new_id
lspci -vvd:37c9
```

Another way to bind the VFs to the DPDK UIO driver is by using the `dpdk-devbind.py` script:

```
cd to the top-level DPDK directory
./usertools/dpdk-devbind.py -b igb_uio 0000:03:01.1
```

## 14.11 Debugging

There are 2 sets of trace available via the dynamic logging feature:

- `pmd.qat_dp` exposes trace on the data-path.
- `pmd.qat_general` exposes all other trace.

`pmd.qat` exposes both sets of traces. They can be enabled using the log-level option (where 8=maximum log level) on the process cmdline, e.g. using any of the following:

```
--log-level="pmd.qat_general,8"
--log-level="pmd.qat_dp,8"
--log-level="pmd.qat,8"
```

---

**Note:** The global `RTE_LOG_DP_LEVEL` overrides data-path trace so must be set to `RTE_LOG_DEBUG` to see all the trace. This variable is in `config/rte_config.h` for meson build and `config/common_base` for gnu make. Also the dynamic global log level overrides both sets of trace, so e.g. no QAT trace would display in this case:

```
--log-level="7" --log-level="pmd.qat_general,8"
```

---

## VIRTIO CRYPTO POLL MODE DRIVER

The virtio crypto PMD provides poll mode driver support for the virtio crypto device.

### 15.1 Features

The virtio crypto PMD has support for:

Cipher algorithms:

- `RTE_CRYPTO_CIPHER_AES_CBC`

Hash algorithms:

- `RTE_CRYPTO_AUTH_SHA1_HMAC`

### 15.2 Limitations

- Only supports the session-oriented API implementation (session-less APIs are not supported).
- Only supports modern mode since virtio crypto conforms to virtio-1.0.
- Only has two types of queues: data queue and control queue. These two queues only support indirect buffers to communication with the virtio backend.
- Only supports AES\_CBC cipher only algorithm and AES\_CBC with HMAC\_SHA1 chaining algorithm since the vhost crypto backend only these algorithms are supported.
- Does not support Link State interrupt.
- Does not support runtime configuration.

### 15.3 Virtio crypto PMD Rx/Tx Callbacks

Rx callbacks:

- `virtio_crypto_pkt_rx_burst`

Tx callbacks:

- `virtio_crypto_pkt_tx_burst`

## 15.4 Installation

Quick instructions are as follows:

Firstly run DPDK vhost crypto sample as a server side and build QEMU with vhost crypto enabled. QEMU can then be started using the following parameters:

```
qemu-system-x86_64 \
[...] \
  -chardev socket,id=charcrypto0,path=/path/to/your/socket \
  -object cryptodev-vhost-user,id=cryptodev0,chardev=charcrypto0 \
  -device virtio-crypto-pci,id=crypto0,cryptodev=cryptodev0
[...]
```

Secondly bind the `uio_generic` driver for the `virtio-crypto` device. For example, `0000:00:04.0` is the domain, bus, device and function number of the `virtio-crypto` device:

```
modprobe uio_pci_generic
echo -n 0000:00:04.0 > /sys/bus/pci/drivers/virtio-pci/unbind
echo "1af4 1054" > /sys/bus/pci/drivers/uio_pci_generic/new_id
```

Finally the front-end `virtio crypto` PMD driver can be installed:

```
cd to the top-level DPDK directory
sed -i 's,\(CONFIG_RTE_LIBRTE_PMD_VIRTIO_CRYPT0\) =n,\1=y,' config/common_base
make config T=x86_64-native-linuxapp-gcc
make install T=x86_64-native-linuxapp-gcc
```

## 15.5 Tests

The unit test cases can be tested as below:

```
reserve enough huge pages
cd to the top-level DPDK directory
export RTE_TARGET=x86_64-native-linuxapp-gcc
export RTE_SDK=`pwd`
cd to test/test
type the command "make" to compile
run the tests with "./test"
type the command "cryptodev_virtio_autotest" to test
```

The performance can be tested as below:

```
reserve enough huge pages
cd to the top-level DPDK directory
export RTE_TARGET=x86_64-native-linuxapp-gcc
export RTE_SDK=`pwd`
cd to app/test-crypto-perf
type the command "make" to compile
run the tests with the following command:

./dpdk-test-crypto-perf -l 0,1 -- --devtype crypto_virtio \
  --ptest throughput --optype cipher-then-auth --cipher-algo aes-cbc \
  --cipher-op encrypt --cipher-key-sz 16 --auth-algo sha1-hmac \
  --auth-op generate --auth-key-sz 64 --digest-sz 12 \
  --total-ops 100000000 --burst-sz 64 --buffer-sz 2048
```



## ZUC CRYPTO POLL MODE DRIVER

The ZUC PMD (`librte_pmd_zuc`) provides poll mode crypto driver support for utilizing Intel Libsso library, which implements F8 and F9 functions for ZUC EEA3 cipher and EIA3 hash algorithms.

### 16.1 Features

ZUC PMD has support for:

Cipher algorithm:

- `RTE_CRYPTOP_CIPHER_ZUC_EEA3`

Authentication algorithm:

- `RTE_CRYPTOP_AUTH_ZUC_EIA3`

### 16.2 Limitations

- Chained mbufs are not supported.
- ZUC (EIA3) supported only if hash offset field is byte-aligned.
- ZUC (EEA3) supported only if cipher length, cipher offset fields are byte-aligned.
- ZUC PMD cannot be built as a shared library, due to limitations in the underlying library.

### 16.3 Installation

To build DPDK with the ZUC\_PMD the user is required to download the export controlled `libsso_zuc` library, by registering in [Intel Resource & Design Center](#). Once approval has been granted, the user needs to search for *ZUC 128-EAA3 and 128-EIA3 3GPP cryptographic algorithms Software Library* to download the library or directly through this [link](#). After downloading the library, the user needs to unpack and compile it on their system before building DPDK:

```
make
```

## 16.4 Initialization

In order to enable this virtual crypto PMD, user must:

- Export the environmental variable LIBSSO\_ZUC\_PATH with the path where the library was extracted (zuc folder).
- Export the environmental variable LD\_LIBRARY\_PATH with the path where the built lib-sso library is (LIBSSO\_ZUC\_PATH/build).
- Build the LIBSSO\_ZUC library (explained in Installation section).
- Build DPDK as follows:

```
make config T=x86_64-native-linuxapp-gcc
sed -i 's,\(CONFIG_RTE_LIBRTE_PMD_ZUC\) =n,\1=y,' build/.config
make
```

To use the PMD in an application, user must:

- Call `rte_vdev_init("crypto_zuc")` within the application.
- Use `-vdev="crypto_zuc"` in the EAL options, which will call `rte_vdev_init()` internally.

The following parameters (all optional) can be provided in the previous two calls:

- `socket_id`: Specify the socket where the memory for the device is going to be allocated (by default, `socket_id` will be the socket where the core that is creating the PMD is running on).
- `max_nb_queue_pairs`: Specify the maximum number of queue pairs in the device (8 by default).
- `max_nb_sessions`: Specify the maximum number of sessions that can be created (2048 by default).

Example:

```
./l2fwd-crypto -l 1 -n 4 --vdev="crypto_zuc,socket_id=0,max_nb_sessions=128" \
-- -p 1 --cdev SW --chain CIPHER_ONLY --cipher_algo "zuc-eea3"
```