Release Note for Intel Communications Chipset 8925 to 8955 Series Software

FreeBSD package version QAT.B.3.0.4-50.tar.gz August 2017

The documentation for this production release is provided in this note. It can be read in conjunction with these documents:

- Intel® Communications Chipset 8925 to 8955 Series Software - Programmer's Guide
- Intel® Communications Chipset 89xx Series Software for Linux – Getting Started Guide

Release Overview

The QAT R3.0.4 FreeBSD package is provided as production quality release intended to be used in production environments. The release supports all QAT Cryptographic services for Chipset 89xx. The QAT R3.0.4 FreeBSD release is fully validated in User Space for FreeBSD 11 64bit. For SRIOV FBSD is support as a guest O/S, with Linux and Xen validated as host platforms.

Environmental Assumptions

The following assumptions are made with regard to the deployment environment

- The driver object/executable file on disk should be protected using the normal file protection mechanisms so that it is writable only by trusted users, for example, a privileged user or an administrator.
- The public key firmware image on disk should be protected using normal file protection mechanisms so that it is writable only by trusted users, for example, a privileged user or an administrator.
- The QAT device should not be exposed (via SR-IOV) to untrusted guests.
- The QAT device should not be exposed (via the "user space direct" deployment model) to untrusted users.
- DRAM is considered to be inside the trust boundary. The normal memory protection schemes provided by the Intel® architecture processor and memory controller, and by the operating system, prevent unauthorized access to these memory regions.
- Persistent keys were not considered, but the storage media are also considered inside the cryptographic boundary.

Limitations with this production release:

- Compression is not supported
- Responses retrieval in interrupt mode is not supported
- Device Utilization feature is not supported
- Rate Limiting is not supported
- Heartbeat is not supported in this release
- NRGB is not supported
- A Kernel Space Driver is not supported
- A 32bit driver is not supported
- Driver not supported in FreeBSD SRIOV host

There are known issues with this release of the driver as described in **After system boot, bring up the driver:**

 # cd /root/QAT/build

./adf_ctl up

Known Issues for Intel® Communications Chipset 8925 to 8955 Series

.

Package Versions

The following table shows the OS-specific package version for each platform supported in this release

Chipset of SoC	Package Version
Intel® Communications Chipset 8925 to 8955 Series	QAT.B.3.0.4-50.tar.gz

MD5 Checksum Information

The table below gives MD5 checksum information.

	Package	Checksum
QAT Package	QAT.B.3.0.4-50.tar.gz	a4b6d2dcf43c08a3631f6e2aa50ad2c0

Licensing for Linux* Acceleration Software

The acceleration software is provided under the following license as listed in the table below. When using or redistributing dual-licensed components, you may do so under either license.

Component	Licence	Directories
User Space Library	BSD	./quickassist/build_system ./quickassist/include ./quickassist/lookaside ./quickassist/utilities/osal
Kernel space driver	Dual BSD/GPL v2	./quickassist/qat/drivers ./quickassist/utilities/adf_ctl
Compatibility layer for older kernel versions	GPL	./quickassist/qat/compat
User Space DMA-able Memory Driver	Dual BSD/GPL v2	./quickassist/utilities/libusdm
libcrypto	OpenSSL	./quickassist/utilities/osal/src/linux/user_space/openssl
CPM Firmware	Redistribution	./quickassist/qat/fw

QuickAssist Driver Package Installation on FreeBSD Environment

The user must have root privileges to perform the following instructions. The user can install the driver to a custom location and "/root/QAT" is used within these instructions as an example installation location.

1) Compiling the Driver

Step 1: Copy package onto the system.

Step 2: Extract package.

```
# cd /root/
# mkdir QAT
# cd QAT
# tar -xzomf <path_to>/ QAT.B.3.0.4-50.tar.gz
```

Step 3: Set network proxy (if required) and install dependencies.

```
gmake:
# setenv http_proxy http://<proxy_server>:<proxy_port>
# cd /usr/ports/devel/gmake
# make config-recursive
# make install

Boost Libraries:
# cd /usr/ports/devel/boost-libs/
# make config-recursive
# make install
```

Step 4: Setup the environment to build driver.

```
# /root/QAT/
# source ./configure.sh
```

Step 5: Build and install driver

```
# gmake install
```

Step 6: Bring up the driver

```
# cd build
# ./adf_ctl up
```

2) Compiling and execute performance sample code

Step 1: Build application

```
# cd /root/QAT/
# gmake sample_code
```

Step 2: Run application

```
# cd ./build
# ./cpa_sample_code signOfLife=1  <- sign of life tests
# ./cpa_sample_code               <- full application run
```

3) Uninstalling the driver

Step 1: Bring down the driver

```
# ./adf_ctl down
```

Step 2: Uninstall driver

```
# cd /root/QAT/
# gmake uninstall
```

4) Making the driver persistent

Step 1: Add the following to /boot/loader.conf:

```
qat_895xcc_mmp.bin_load="YES"
qat_common_load="YES"
qat_dh895xcc_load="YES"
qat_dh895xccvf_load="YES"
qae_mem_load="YES"
```

Step 2: After system boot, bring up the driver:

```
# cd /root/QAT/build
# ./adf_ctl up
```

Known Issues for Intel® Communications Chipset 8925 to 8955 Series

The known issue additions or updates since the last release of the software for the platform are listed below.

Summary of Known Issues for Intel® Communications Chipset 8925 to 8955 Series

QATE-5092	CY: AES-XTS does not support buffers sizes that are not a multiple of 16B
QATE-7325	CY: AES-GCM operation with zero length plain text results in an incorrect tag result
QATE-10019	Gen: The mmaped CSR region in user space is not unmaped at the end
QATE-10386	The icp_sal_reset command to a device influences behaviour of other devices

Title	CY: AES-XTS does not support buffers sizes that are not a multiple of 16B
Reference #	QATE-5092
Description	A single request with a data size that is not a multiple of 16B for AES-XTS will fail in the IA QuickAssist driver with an invalid param check.
Implication	The user cannot submit AES-XTS Crypto requests with buffers that are not multiples of 16B.
Resolution	No Workaround Available
Affected OS	FreeBSD 8.x
Driver/ Module	CPM IA – Crypto

Title	CY: AES-GCM operation with zero length plain text results in an incorrect tag result
Reference #	QATE-7325
Description	Sending an AES-GCM operation with zero length plain text to Cave Creek using the Quick Assist API results in an incorrect tag result
Implication	Potentially bad record errors and failing connections
Resolution	There is no workaround available
Affected OS	FreeBSD 8.x
Driver/ Module	Feature - Acceleration Driver

Title	Gen: The mmaped CSR region in user space is not unmaped at the end
Reference #	QATE-10019
Description	If creating (or forking a process) and mapping rings into process, the process can crash. This happens mostly when high process creation / disposal rate is made.
Implication	The process can crash
Resolution	Do not create processes dynamically
Affected OS	FreeBSD 8.x
Driver/ Module	Feature - Acceleration Driver

Title	The icp_sal_reset command to a device influences behaviour of other devices
Reference #	QATE-10386
Description	When calling icp_sal_reset_device(Cpa32U accelId), all the processes accessing any QAT device (even not the one being reset) should be quiescently stopped and recover after reset. The sample code providing the workflow during icp_sal_reset_device is provided in sample_code folder.
Implication	Other devices stop working
Resolution	There is no workaround available
Affected OS	FreeBSD 8.x
Driver/ Module	Feature - Acceleration Driver