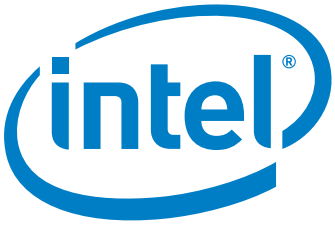

Intel® QuickAssist Technology Software for Linux*

Release Notes

February 2018

Package Version: QAT1.7.L.1.0.3-42.tar.gz

Document Number: 336211-003

Contents

Tables

Revision History

Released Revision History

Date	Revision	Description
February 2018	003	For software release 1.0.3-42 **New Open Issues:** • QATE-13822 and QATE-13823 **Revised Open Issue:** • QATE-9953 now includes both static and dynamic compression.
August 2017	002	For software release 1.0.3-42
July 2017	001	Initial product release

Pre-release Revision History

Date	Revision	Description
July 2017	0.97	For software release 1.0.3-42 Updated package number and checksum. **New Open Issues:** • QATE-9953
May 2017	0.96	For software release 1.0.3 Updated package number and checksum. **New Open Issues:** • QATE-9241, QATE-9234, QATE-9326 and QATE-8233 **Newly Resolved Issues:** • QATE-3650, QATE-3259 and QATE-8189
May 2017	0.95	For software release 1.0.2 Updated package number and checksum. Updated generic collateral website link. **New Open Issues:** • QATE-8361, QATE-8189 and QATE-8109 **Newly Resolved Issues:** • QATE-7909
April 2017	0.94	For software release 1.0.1 Updated package number, checksum, and instructions for obtaining SoC BIOS
March 2017	0.93	Updated instructions for obtaining SoC BIOS
March 2017	0.92	For software release 1.0 Updated software license locations in Table 4. **New Open Issues:** • QATE-5989 and QATE-7393 **Newly Resolved Issues:** • QATE-3017
February 2017	0.91	Updated BIOS information for SoC Updated list of unsupported features All open and resolved issues have new reference numbers **New Open Issues:** • QATE-4051, QATE-5433, and QATE-3017 **Newly Resolved Issues:** • QATE-3220, QATE-3072, QATE-2985, QATE-4015 and QATE-6463

§

1.0 Description of Release

This document describes extensions and deviations from the release functionality described in the software Programmer's Guides for the various platforms that support Intel® QuickAssist Technology.

Changes in this software release include:

Standard Linux* installation support added

For instructions on loading and running the release software, see the Getting Started Guide for your platform (see Section 1.5, "Related Documentation" on page 9).

Note: This software release is intended for platforms that contain:

- Intel® C62x Chipset
- Intel Atom® C3000 Processor Product Family
- Intel® Xeon® Processor D Family
- Intel® QuickAssist Adapter 8960/Intel® QuickAssist Adapter 8970 (formerly known as "Lewis Hill")

These release notes may also include known issues with third-party or reference platform components that affect the operation of the software.

1.1 Features/Limitations

The main features available on platforms using Intel® QuickAssist Technology are:

- Cryptographic services
- Data compression services
- Cryptographic sample applications
- Data Compression Sample Applications
- Intel® QuickAsssist Technology Data Plane Cryptographic API (`cpa_cy_sym_dp.h`)
- Intel® QuickAsssist Technology Data Plane Data Compression API (`cpa_dc_dp.h`)

The following features are not currently supported:

- Heartbeat
- Dynamic instances

1.2 Supported Operating Systems

The software in this release has been validated with CentOS* (64-bit) for the following products:

- Intel® C62x Chipset
- Intel Atom® C3000 Processor Product Family
- Intel® Xeon® Processor D Family
- Intel® QuickAssist Adapter 8960/Intel® QuickAssist Adapter 8970 (formerly known as "Lewis Hill")

It has been validated with Yocto* for this product:

Intel Atom® C3000 Processor Product Family

Note: While the Intel® QuickAssist Accelerator software is validated on CentOS 7, it should work without change on some other Linux* distributions and kernels.

1.2.1 Version Numbering Scheme

The software is provided in a top-level package that contains sub-packages for the various supported platforms.

The version numbering scheme for all package levels is similar:

```
name.os.major.minor.maintenance-build
```

Where:

- `name` is the name of the package:
  For the top-level package, the name is "QAT1.7.Upstream"
- `os` is the operating system, in all cases, "Linux*"
- `major` is the major version of the software
- `minor` is the minor version of the software
- `maintenance-build` is the maintenance release and build number

1.2.2 Package Versions

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

Table 1. Package Versions

Chipset or SoC	Package Version
Top-Level Package	QAT1.7.L.1.0.3-42.tar.gz

1.2.3 Licensing for Linux* Acceleration Software

The acceleration software is provided under the licenses listed in Table 2. When using or redistributing dual-licensed components, you may do so under either license.

Table 2. Linux* Acceleration Software Licensing Files

Component	License	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
Boost library used to help parse the config file	Boost	./quickassist/utilities/adf_ctl/third_party/boost
libcrypto	OpenSSL	./quickassist/utilities/osal/src/linux/user_space/openssl
CPM Firmware	Redistribution	./quickassist/qat/fw
Calgary corpus and Canterbury corpus test files	Public domain	./quickassist/lookaside/access_layer/src/sample_code

1.2.4 BIOS/Firmware Version

The term BIOS is used to refer to the pre-boot firmware that could include legacy BIOS or Extensible Firmware Interface (EFI) compliant firmware.

Note: Update your platform so it uses the latest available version of the BIOS/firmware available for that platform.

For the Intel C62x Chipset, update your Purley platform to use the BIOS/firmware version available through Purley BKC for that platform.

Development Platform	BIOS/Firmware Version
Long Brook	LBRFCRB1.86B.0259.D07.1509171304
Taliverde	TVD.B0PO.SPS.02.027.RC34.NVM.2.13.ReleaseSS

For the Intel Atom® C3000 Processor Product Family and the Intel® Xeon® Processor D Family:

Development Platform	BIOS/Firmware Version
Harcuvar w/ B0	refer to Intel® Business Link (IBL) - 562202
Harcuvar w/ B1	refer to Intel® Business Link (IBL) - 562202

1.2.4.1 MD5 Checksum Information

The table below gives MD5 checksum information.

	Package	Checksum
Main Package	QAT1.7.L.1.0.3-42.tar.gz	ee059cf134486f5684466555e8636ee0

1.3 Intel® QuickAssist Technology API Updates

Note: The QAT API version number is different from the software package version number.

For details on any changes to the Intel® QuickAssist Technology APIs, refer to the Revision History pages in the following API reference manuals:

- *Intel® QuickAssist Technology Cryptographic API Reference Manual API Version 2.01*
- *Intel® QuickAssist Technology Data Compression API Reference Manual API Version 2.0*
- *Intel®QuickAssist Technology Software Pre-Release - Hardware Version 1.7 - Documentation Addendum*

1.4 Technical Support

Intel offers support for this software at the API level only, defined in the programmer's guides and API reference manuals listed in Section 1.5. If your field representative has created an account for you, support requests can be submitted via https://premier.intel.com.

1.5 Related Documentation

Table 3 lists Intel® QuickAssist Technology generic documentation.

Table 3. Intel® QuickAssist Technology Generic Documentation

Document Name	Reference Number
Intel® QuickAssist Technology API Programmer's Guide	330684
Intel® QuickAssist Technology Cryptographic API Reference Manual	330685
Intel® QuickAssist Technology Data Compression API Reference Manual	330686
Intel® QuickAssist Technology Performance Optimization Guide	330687
Using Intel® Virtualization Technology (Intel® VT) with Intel® QuickAssist Technology Application Note	330689

Table 4 lists Intel® QuickAssist Technology specific documentation.

Table 4. Intel® QuickAssist Technology Software Specific Documentation

Document Name	Reference Number
Intel® QuickAssist Technology Software for Linux Getting Started Guide - Hardware Version 1.7*	336212
Intel® QuickAssist Technology Software for Linux Software Programmer's Guide - Hardware Version 1.7*	336210

1.6 Terminology

Table 5 lists Intel® QuickAssist Technology acronyms.

Table 5. Acronyms

Acronym	Definition
CY	Cryptographic component
DC	Compression component
QAT	Intel® QuickAssist Technology
SRIOV	Single Root I/O Virtualization component

§

2.0 Where to Find Current Software

Collateral can be found on https://01.org/intel-quickassist-technology

2.1 Accessing Additional Content from the Intel Business Portal

1. In a web browser, go to www.intel.com/ibl.
2. Enter your login ID in the **Login ID** box. Check **Remember my login ID** only if you are not using a shared computer. Click **Submit**.

Note: To acquire a new Intel Business Portal account, please contact your Intel Field Sales Representative.

3. Enter your password in the **Password** box. Click **Submit**.
4. **For the Intel® C62x Chipset PCH**: Within the design kit categories, under the **Platform & Solutions** heading, click **Server and Workstation**. Under the **Products** heading, click **Server and Workstation Platforms Codenamed Purley, including Skylake Server and Cannonlake Server processors, with Lewisburg PCH** then, under the Associated Collateral Lists heading, click **Server and Workstation Platforms: Purley - Lewisburg Chipset Intel QuickAssist Technology Software**
   (Then continue to step 6.)
5. **For the Intel Atom® C3000 Processor Product Family SoC**:Within the design kit categories, under the **Platform & Solutions** heading, click **Embedded**. Under the **Pre-Launch Products** heading, click **Embedded Platform Code Named Denverton-NS** then, under the Associated Collateral Lists heading, click **Microserver Platform Code Named Harrisonville – Denverton and Denverton-NS Intel QuickAssist Technology Software**
6. The collateral lists contains the acceleration driver package (562366), together with the product documentation listed in Table 3.
7. Save the file(s) in the directory of your choice.
8. Unpack and install the software using the instructions in your platform's Getting Started Guide.

2.2 List of Files in Release

The Bill of Materials, sometimes referred to as the BOM, is included as a text file in the released software package. This text file is labeled `filelist` and is located at the top directory level for each release.

§

3.0 Intel® QuickAssist Technology Software - Issues

Known and resolved issues relating to the Intel® QuickAssist Technology software are described in this section.

Note: Issue titles follow the pattern **Identifier - <Component> [Stepping] : Description of issue** where:

<Component> is one of the following:

- CY - Cryptographic
- DC - Compression
- EP - Endpoint
- GEN - General
- SYM DP - Symmetric Cryptography on Data Plane
- SRIOV - Single Root I/O Virtualization
- FIRM - Firmware

[Stepping] is an optional qualifier that identifies if the errata applies to a specific device stepping.

3.1 Known Issues

Table 6. Summary of Known Issues

3.1.1 QATE-3982 - GEN - Child process crashes as it is accessing Parent process's address space

Title	**GEN - Child process crashes as it is accessing Parent process's address space**
Reference #	QATE-3982
Description	Parent process calls icp_sal_userStartMultiProcess() which allocates memory for all rings. When a Child process subsequently calls icp_sal_userStartMultiProcess() the memory for rings is not remapped.Thus when a Child process starts a polling thread and tries to access the rings, it crashes as it is accessing Parent process's address space.
Implication	Child process crash
Resolution	There is no workaround available
Affected OS	Linux
Driver/Module	QAT_1.7 Upstreamed Driver CPM IA - Common

3.1.2 QATE-3039 - Gen - Build fails when system time is set too far in the past, relative to the package -

Title	**Gen - Build fails when system time is set too far in the past, relative to the package**
Reference #	QATE-3039
Description	Extract the package on a system on which the system time is not set correctly and attempt to build it. The build fails.
Implication	The build fails
Resolution	Update System Time
Affected OS	Linux
Driver/Module	QAT_1.7 Upstreamed Driver Seamless Installation

3.1.3 QATE-4111 - DC - Lewisburg/Denverton: Engine timeout not handled correctly -

Title	**DC - Lewisburg/Denverton: Engine timeout not handled correctly**
Reference #	QATE-4111
Description	When an engine timeout occurs due to watchdog expiration, compression engines might lock up.
Implication	In some rare conditions, the compression engine might become unresponsive.

Title	**DC - Lewisburg/Denverton: Engine timeout not handled correctly**
Resolution	Reset the device if it is unresponsive. A reset sequence can be triggered by running adf_ctl down followed by adf_ctl up.
Affected OS	Linux
Driver/Module	CPM FW - Data Compression

3.1.4 QATE-4051 - GEN - Lewisburg/Denverton: Full device pass-through not available on KVM guests. -

Title	**GEN - Lewisburg/Denverton: Full device pass-through not available on KVM guests.**
Reference #	QATE-4051
Description	The new firmware authentication feature in Lewisburg/Denverton requires PF devices to be reset via function level reset (FLR) before firmware download. In KVM guests, all pass-through devices attached to a VM are reset at boot time. Any further device reset is trapped by the hypervisor and not issue. This causes firmware authentication to fail after the first firmware download. Full device pass-through works if using vfio and if the host kernel and the platform support it.
Implication	Direct mode feature not available on KVM guests for Lewisburg/Denverton devices on full pass-through mode.
Resolution	This requires a fix in QEMU to allow a guest to perform a function level reset
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.5 QATE-5433 - GEN - User space library supports only 32 devices -

Title	**GEN - User space library supports only 32 devices**
Reference #	QATE-5433
Description	The user space library enumerates only the first 32 devices in the system.
Implication	In a system with more than 32 devices, the devices indexed at and higher than 32 are unusable.As a consequence of this, when running an application, the application will only use 32 devices even if there are more than 32 started.
Resolution	If more than 32 devices are needed, the user can remove the redefinition of ADF_MAX_DEVICES in quickassist/lookaside/access_layer/src/qat_direct/include/icp_adf_init.h (lines 53 to 56) and re-install the driver.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.6 QATE-3628 - GEN - Lewisburg/Denverton: slice hang not reported in syslog -

Title	**GEN - Lewisburg/Denverton: slice hang not reported in syslog**
Reference #	QATE-3628
Description	When a slice hang condition occurs, an error is reported to the user exclusively in the call-back of the job that triggered that condition. The error is not reported in the system log.
Implication	It is not possible to monitor slice hang conditions using system log.
Resolution	There is no workaround available.
Affected OS	Linux
Driver/Module	ADF - Kernel Mode

3.1.7 QATE-3635 - SRIOV - VFs cannot be cleanly disabled on acceleration device -

Title	**SRIOV - VFs cannot be cleanly disabled on acceleration device**
Reference #	QATE-3635
Description	Writing 0 to /sys/bus/pci/devices/<BDF>/sriov_numvfs results in no action.
Implication	Virtual functions cannot be disabled by writing 0 to /sys/bus/pci/devices/ <BDF>/sriov_numvfs.
Resolution	Virtual functions can be disabled through adf_ctl down on the PF.
Affected OS	Linux
Driver/Module	ADF - Kernel Mode

3.1.8 QATE-3241 - CY - cpaCySymPerformRequest when used with parameter checking may reveal the amount of padding. -

Title	**CY - cpaCySymPerformRequest when used with parameter checking may reveal the amount of padding.**
Reference #	QATE-3241
Description	When Performing a CBC Decryption as a chained request using cpaCySymPerformRequest it is necessary to pass a length of the data to MAC (messageLenToHashInBytes). With ICP_PARAM_CHECK enabled, this checks the length of data to MAC is valid and if not it aborts the whole operation and outputs an error on stderr.
Implication	The length of the data to MAC is based on the amount of padding. This should remain private and not be revealed. This is not an issue if the length is checked in constant time before passing the value to the API. This is done by OpenSSL.
Resolution	1) Build without ICP_PARAM_CHECK, but this opens the risk of buffer overrun. Or 2) Validate the length before using the API.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.1.9 QATE-5989 - CY -AES-GCM operations with zero length plain text results in an incorrect tag result -

Title	**CY -AES-GCM operations with zero length plain text results in an incorrect tag result**
Reference #	QATE-5989
Description	Sending an AES-GCM operation with zero length plain text using the Quick Assist API results in an incorrect tag result.
Implication	Incorrect result when computing AES-GCM for zero length payloads.
Resolution	Zero length AES-GCM requests should be submitted as GMAC.
Affected OS	Linux
Driver/Module	OS Compatibility

3.1.10 QATE-7393 - CY - AES-CCM operations with zero length plain text results in an incorrect tag result -

Title	**CY - AES-CCM operations with zero length plain text results in an incorrect tag result**
Reference #	QATE-7393
Description	Sending an AES-CCM operation with zero length plain text using the Quick Assist API results in an incorrect tag result.
Implication	Incorrect result when computing AES-CCM for zero length payloads.
Resolution	Set messageLenToHashInBytes to 0 in CpaCySymOpData when sending an AES-CCM zero-length request.
Affected OS	Linux
Driver/Module	OS Compatibility

3.1.11 QATE-8361 - GEN - ICP_WITHOUT_THREAD not supported -

Title	**GEN - ICP_WITHOUT_THREAD not supported**
Reference #	QATE-8361
Description	The software package no longer supports the ICP_WITHOUT_THREADS build flag.
Implication	It is not possible to build a version of the software package without a dependency with the pthread library. The pthread library is used only for synchronization purposes. User space threads are not created.
Resolution	There is no workaround available.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.12 QATE-8109 - GEN - Driver and firmware versions are not reported to user space -

Title	**GEN - Driver and firmware versions are not reported to user space**
Reference #	QATE-8109
Description	Driver and firmware versions are not reported through the sysfs and cannot be queried using the icp api.
Implication	User applications are not able to query the software package versions.
Resolution	There is no workaround available.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.13 QATE-8233 - GEN - Installation of QAT software on Yocto or Ubuntu image results in QAT libraries not being placed in default system path -

Title	**GEN - Installation of QAT software on Yocto or Ubuntu image results in QAT libraries not being placed in default system path**
Reference #	QATE-8233
Description	The qat shared library (libqat_s.so) may be installed somewhere other than the default directory.
Implication	Applications may fail to link to the qat library at run time.This has been observed with Yocto images and Ubuntu 15 and 16.
Resolution	Add the directory where the qat library is installed (normally /lib64) to the LD_LIBRARY_PATH environment variable.Alternatively, copy or link the qat library from the installed directory to the default shared library directory.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.14 QATE-9234 - GEN - Child process should not inherit mapping to QAT rings -

Title	**GEN - Child process should not inherit mapping to QAT rings**
Reference #	QATE-9234
Description	If a process forks after calling icp_sal_userStart, when the child process exits, the syslog will show a message "Process <PID> <NAME> exit with orphan rings"
Implication	None
Resolution	There is no workaround available.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.15 QATE-9326 - DC - Changing StorageEnabled back to 0 doesn't reload FW -

Title	**DC - Changing StorageEnabled back to 0 doesn't reload FW**
Reference #	QATE-9326
Description	If the configuration file is modified to change StorageEnabled from 1 to 0, this does not cause the storage firmware to be replaced to the standard one.
Implication	PKE functions will not work after changing StorageEnabled from 1 to 0.
Resolution	Remove and reload the kernel module after changing the StorageEnabled configuration from 1 to 0.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.16 QATE-9241 - GEN - Process exit with orphan rings when spawning multiple processes -

Title	**GEN - Process exit with orphan rings when spawning multiple processes**
Reference #	QATE-9241
Description	If multiple processes start a user space service access layer (icp_sal_userStart) and they all exit together, the syslog may show a message "Process <PID> <NAME> exit with orphan rings"
Implication	None
Resolution	There is no workaround available.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.17 QATE-9483 - GEN - uncorrectable errors might lead to a kernel panic -

Title	**GEN - uncorrectable errors might lead to a kernel panic**
Reference #	QATE-9483
Description	If an uncorrectable error is triggered when there are in flight requests, the system might crash and report kernel panic.
Implication	If this error occurs, the system must be rebooted
Resolution	There is no workaround available.
Affected OS	Linux
Driver/Module	ADF - Kernel Mode

3.1.18 QATE-9953 - DC: Static and Dynamic compression may lead to data loss -

Title	**DC: Static and Dynamic compression may lead to data loss**
Reference #	QATE-9953
Description	In rare cases the compression feature will result in the inability to recreate the original data from the compressed data. This issue affects both Static and Dynamic compression.
Implication	Data compressed with the Static or Dynamic compression feature in rare cases will result in the inability to recreate the original data from the compressed data.
Resolution	Intel is requiring that customers verify data integrity when using either Static or Dynamic compression. Customers should decompress the data and verify that it matches the original source data when using Static or Dynamic compression. In the storage specific firmware Intel provides these APIs that perform "Compress and Verify": cpaDcCompressData2(…) cpaDcDpEnqueueOp(…) with compressAndVerify and cpaDcDpEnqueueOpBatch(…) with compressAndVerify If customers are not using the above APIs then they must verify the compressed data can be decompressed to the original data before using the compressed data.
Affected OS	Linux
Driver/Module	QAT_1.7 Upstreamed Driver CPM FW - Data Compression

3.1.19 QATE-9806 - GEN - Throughput and Ratio stats not outputted for BnP sample code -

Title	**GEN - Throughput and Ratio stats not outputted for BnP sample code**
Reference #	QATE-9806
Description	Required output data is incomplete
Implication	It is not possible to assess the performance of Batch and Pack feature
Resolution	There is no workaround available.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.20 QATE-13823 - DC: "Batch and Pack" APIs are deprecated -

Title	**DC: "Batch and Pack" APIs are deprecated**
Reference #	QATE-13823

Description	Intel is deprecating the Batch and Pack data compression APIs:
	`cpaDcBPCompressData(..)`
	`cpaDcBnpBufferListGetMetaSize(..)`

Implication	Future releases of QAT Driver will not provide the Batch and Pack feature.

Title	DC: "Batch and Pack" APIs are deprecated
Resolution	Applications using Batch and Pack APIs need to migrate to the other compression APIs.
Affected OS	Linux
Driver/Module	QAT_1.7 Upstreamed Driver - Data Compression

3.1.21 QATE-13822 - DC: Stateful compression is deprecated -

Title	DC: Stateful compression is deprecated
Reference #	QATE-13822
Description	Intel is deprecating stateful compression.
Implication	Future releases of QAT Driver will return an error when the CPA_DC_STATEFUL enumeration is used in compression requests.
Resolution	Applications using CPA_DC_STATEFUL need to migrate to CPA_DC_STATELESS for compression session creation.
Affected OS	Linux
Driver/Module	QAT_1.7 Upstreamed Driver - Data Compression

3.2 Resolved Issues

Table 7. Summary of Resolved Issues

3.2.1 QATE-3369 - DC - Increased minimum destination buffer size for compression -

Title	**DC - Increased minimum destination buffer size for compression**
Reference #	QATE-3369
Description	During the compression of a request that is a multiple of 8 bytes in length (compress a file 1024 bytes long) extra work must be done to validate that no data is lost as the end of the request.
Implication	The implication of this workaround is that the minimum compression destination buffer size has increased from 64 bytes to 96 bytes. The new minimum destination buffer size (96B) must be used for all compression requests (static and dynamic compression, stateful and stateless)
Resolution	Allocate a destination buffer size of at least 96 bytes for compression jobs
Affected OS	Linux
Driver/Module	CPM FW - Data Compression

3.2.2 QATE-3683 - DC - Stateful Decompression Returns -13 Error with Negative Test (A step silicon only) -

Title	**DC - Stateful Decompression Returns -13 Error with Negative Test (A step silicon only)**
Reference #	QATE-3683
Description	If incorrectly formatted data is fed to the hardware, the API may return a status of -13 (CPA_DC_FATALERR). This error means that the session needs to be restarted but the device does not need to be reset.
Implication	For stateful decompression if the input content is invalid both a -10 soft error and a -13 hard error are reported. Only the hard error is sent back to driver as the hard error has higher priority.
Resolution	For A step silicon: If an invalid stateful decompression request is sent to the QAT driver and a -13 error code is returned the complete session should be restarted. There is no need to reset the device. This is resolved with B step silicon.
Affected OS	Linux
Driver/Module	CPM IA - Data Compression

3.2.3 QATE-4070 - GEN - The driver fails to send requests if the first ring put operation returns a retry or a failure when using partial symmetric crypto operations -

Title	**GEN - The driver fails to send requests if the first ring put operation returns a retry or a failure when using partial symmetric crypto operations**
Reference #	QATE-4070
Description	The driver can enter a deadlock state due to improper locking when using symmetric crypto operations with partial packets. This occurs when there is heavy traffic and the 1st request receives a retry or a failure when it tries to send a message to the ring.
Implication	When using the application server and using symmetric crypto operations with partial packets then it is possible to receive a retry when trying to send the first request, causing the nonBlockingOpsInProgress to be set to false. The callback function for the 1st response won't be called causing all the requests for this session to be en-queued and none can be de-queued and sent to the ring until the the client and application server stop communicating. The application server has connection leaks when the client send lots of request at the same time. When the client stops sending requests, there are many "active connections" left in the application server.
Resolution	This is resolved with the 0.8.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.4 QATE-4071 - CY - cpaCySymRemoveSession fails in Data Plane API if other active Session sharing ring -

Title	**CY - cpaCySymRemoveSession fails in Data Plane API if other active Session sharing ring**
Reference #	QATE-4071
Description	If multiple sessions are sharing the same Crypto DP instance, then a call to cpaCySymRemoveSession() will fail if there are messages inflight from another session.
Implication	cpaCySymRemoveSession() may fail
Resolution	This is resolved with the 0.8.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.5 QATE-3137 - CY - AES-XTS does not support buffers sizes that are not a multiple of 16B -

Title	**CY - AES-XTS does not support buffers sizes that are not a multiple of 16B**
Reference #	QATE-3137
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.

Title	**CY - AES-XTS does not support buffers sizes that are not a multiple of 16B**
Resolution	This is resolved with the 0.8.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.6 QATE-3715 - CY - Incorrect hash generated with SHA384 and secret length > 64 bytes -

Title	**CY - Incorrect hash generated with SHA384 and secret length > 64 bytes**
Reference #	QATE-3715
Description	An incorrect hash is generated when using SHA384 with secret length greater than 64 bytes. If the secret is length is <= 64 bytes OR the hash algorithm is different from SHA384 the results are correct.
Implication	Don't use secret length of > 64bytes with SHA384
Resolution	This is resolved with the 0.8.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.7 QATE-3791 - GEN - Common Memory Driver incorrectly allocates memory of size between 2MB and 4MB -

Title	**GEN - Common Memory Driver incorrectly allocates memory of size between 2MB and 4MB**
Reference #	QATE-3791
Description	This applies to PCH-NS only. If the included memory driver (qae_mem.ko) is used to allocate a block of pinned memory of a size between 2MB and 4MB, the pointer to the allocated memory returned may be incorrect. The included memory driver does not support allocating a block of memory of 4MB or larger.
Implication	The result of an application using a block of memory between 2MB and 4MB in size is indeterminate. The most likely behavior is segmentation fault in the application using the allocated memory. Attempting to allocate memory of size 4MB or greater using the memory driver will fail.
Resolution	This is resolved with the 0.7.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.8 QATE-3702 - DC - Decompression Failure, empty dynamic block reports -7 error -

Title	DC - Decompression Failure, empty dynamic block reports -7 error
Reference #	QATE-3702
Description	When user submits one or more valid empty dynamic blocks, compression slice returns -7 error code. Software implementations are able to decompress these block(s) successfully. An example of valid empty dynamic block: 04 c0 81 08 00 00 00 00 20 7f eb 13 00 00 ff ff
Implication	A -7 soft error will be reported on valid empty dynamic compressed block(s).
Resolution	This is resolved with the 0.8.0 release.
Affected OS	Linux
Driver/Module	CPM FW - Data Compression

3.2.9 QATE-3978 - GEN - The QuickAssist service must be restarted after a reboot -

Title	GEN - The QuickAssist service must be restarted after a reboot
Reference #	QATE-3978
Description	On a fresh boot after a previous QuickAssist driver installation, a QuickAssist application (e.g. the performance sample code) cannot immediately run.
Implication	The following error is seen: [error] SalStatistics_GetStatEnabled() - : Failed to get statsGeneral from configuration file ADF_UIO_PROXY err: adf_user_subsystemInit: Failed to initialise Subservice SAL [error] SalCtrl_ServiceEventStart() - : Private data is NULL ADF_UIO_PROXY err: adf_user_subsystemStart: Failed to start Subservice SAL [error] SalCtrl_AdfServicesStartedCheck() - : Sal Ctrl failed to start in given time [error] do_userStart() - : Failed to start services ADF_UIO_PROXY err: icp_adf_subsystemUnregister: Failed to shutdown subservice SAL. main():710 Could not start sal for user space
Resolution	This is resolved with the 0.7.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.10 QATE-3981 - GEN - Stress test with concurrent crypto and compression may fail with segfault -

Title	GEN - Stress test with concurrent crypto and compression may fail with segfault
Reference #	QATE-3981
Description	When running crypto, compression, and decompression concurrently, a segmentation fault may be observed. In one case, the segmentation was observed after 7 hours of running the following operations concurrently: * AES256-CBC + SHA512 IMIX * Stateless Deflate 50% compress and 50% decompress
Implication	The application fails with a segmentation fault.

Title	**GEN - Stress test with concurrent crypto and compression may fail with segfault**
Resolution	This is resolved with the 0.8.0 release.
Affected OS	Linux
Driver/Module	Test Code

3.2.11 QATE-3986 - GEN - The included memory driver impacts Tradional API sample code performance -

Title	**GEN - The included memory driver impacts Tradional API sample code performance**
Reference #	QATE-3986
Description	The included memory driver has a large impact of performance of the traditional API sample code.The impact depends on the amount of instances used per device, but it has been observed to be impacted by 50% or more in most cases.
Implication	The performance of the sample code using the traditional API is lower than expected.
Resolution	This is resolved with the 0.8.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.12 QATE-3547 - GEN - Killing a Process May Lead to a Kernel Panic -

Title	**GEN - Killing a Process May Lead to a Kernel Panic**
Reference #	QATE-3547
Description	When a process using the driver is killed or terminates unexpectedly, the buffers associated with the bundle are flushed during the cleanup operation. Due to a race condition between releasing the memory by the included memory driver and flushing the buffers, it can sometimes happen that this causes a kernel panic.
Implication	If this occurs, the system must be rebooted.
Resolution	This is resolved with the 0.8.0 release.
Affected OS	Linux
Driver/Module	Common Memory Driver

3.2.13 QATE-3404 - GEN - The included memory driver fails during memory allocation. -

Title	**GEN - The included memory driver fails during memory allocation.**
Reference #	QATE-3404
Description	During stressful memory allocation the included memory driver may fail with below logs and potential kernel crash: User-space logs: ---------- ------- CMD NUMA fail qaeMemAllocNUMA:737 mmap on memory allocated through ioctl failed Kernel-space logs: ---------- kernel: mem_mmap:528 cannot find meminfo kernel: userMemFree:328 Could not find slab with id: xx
Implication	Memory driver may fail to allocate memory in stress conditions. Reboot is required to continue normal operations.
Resolution	This is resolved with the 0.8.0 release.
Affected OS	Linux
Driver/Module	Common Memory Driver

3.2.14 QATE-4018 - SYM DP - cpaCySymDpEnqueueOpBatch accepts only requests in a batch of the same session -

Title	**SYM DP - cpaCySymDpEnqueueOpBatch accepts only requests in a batch of the same session**
Reference #	QATE-4018
Description	When the package is built with ICP_PARAM_CHECK, cpaCySymDpEnqueueOpBatch accepts only batches of requests for the same session. When requests for different sessions are provided, this API fails returning CPA_STATUS_INVALID parameter and reports the following message: "All session contexts should be the same in the requests".
Implication	It is not possible to use the Data Plane API to submit batches of requests that belongs to different sessions using cpaCySymDpEnqueueOpBatch.
Resolution	This is resolved with the 0.9.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.15 QATE-3073 - GEN - Memory corruption on module verification with kernel versions greater than 4.5 -

Title	**GEN - Memory corruption on module verification with kernel versions greater than 4.5**
Reference #	QATE-3073
Description	Verifying any Linux kernel module signature after loading the acceleration driver on any platform with a Linux kernel 4.5 and onwards, will cause a memory corruption issue. This is due to a bug in the kernel for which a fix has been submitted.
Implication	The memory corruption will likely cause a kernel panic and making the system unusable.

Title	**GEN - Memory corruption on module verification with kernel versions greater than 4.5**
Resolution	Do not load any signed kernel module after loading the acceleration driver. Load the acceleration driver at the very last.
Affected OS	Linux
Driver/Module	ADF - Kernel Mode

3.2.16 QATE-3693 - SRIOV - Incorrect config file for PFs when VFs are enabled in the host -

Title	**SRIOV - Incorrect config file for PFs when VFs are enabled in the host**
Reference #	QATE-3693
Description	When the driver is installed in the Host with option 3 (Install SR-IOV Host Acceleration), an incorrect configuration is installed in the system. This prevents the sample code from running properly.
Implication	When trying to run the sample code in a configuration where VFs are enabled in the host, the sample code might not run properly or report an error message similar to this: [error] SalCtrl_AdfServicesStartedCheck() - : Sal Ctrl failed to start in given time [error] do_userStart() - : Failed to start services main():731 Could not start sal for user space
Resolution	This is resolved with the 0.8.1 release.
Affected OS	Linux
Driver/Module	ADF - User Mode

3.2.17 QATE-3007 - GEN - Unexpected error message when trying to bring up the driver -

Title	**GEN - Unexpected error message when trying to bring up the driver**
Reference #	QATE-3007
Description	The driver reports an error similar to the one below when it is brought up with adf_ctl: Processing /etc/c6xx_dev0.conf Invalid affinity configuration Kernel space instances needs to be allocated on bundles lower than userspace instances Please change CoreAffinity configuration Failed to process section SSL_INT_0 QAT Error: Invalid configuration Failed to configure qat_dev1
Implication	The driver might not be able to load valid V2 configuration files that were correctly loaded by the legacy driver.
Resolution	This is resolved with the 0.9.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.18 QATE-3220 - GEN - Potential Response Data Leak -

Title	**GEN - Potential Response Data Leak**
Reference #	QATE-3220
Description	An internal QAT system resource is being released back to the resource pool before the PRF service has completely finished and it is reused by other service.
Implication	When accelerating TLS PRF (Pseudo Random Function) in parallel with another service (crypto or compression), portions of input data may leak between processes or virtual machines. This is more probable when the system is under stress. For example, when running symmetric crypto encryption in parallel with TLS PRF, portions of the input data sent for encryption might appear in the TLS PRF output buffer without encryption.
Resolution	This is resolved with the 0.9.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.19 QATE-3072 - GEN - Stack dump after first adf_ctl down on a VF -

Title	**GEN - Stack dump after first adf_ctl down on a VF**
Reference #	QATE-3072
Description	After the first adf_ctl down on a VF, the kernel reports on a syslog a call trace which suggests a problem caused by adf_dev_stop.
Implication	Warning reported in syslog. No impact to user.
Resolution	This is resolved with the 0.9.1 release.
Affected OS	Linux
Driver/Module	ADF - Kernel Mode

3.2.20 QATE-2985 - SRIOV - Failed to send response to VF -

Title	**SRIOV - Failed to send response to VF**
Reference #	QATE-2985
Description	When bringing up one or more virtual functions in a host, the driver might report in the system log an error message similar to: "Failed to send response to VF" This is due to a short timeout in the PF2VF protocol.
Implication	Some of the virtual functions might not be available for the host.
Resolution	This is resolved with the 0.9.1 release.
Affected OS	Linux
Driver/Module	ADF - Kernel Mode

3.2.21 QATE-4015 - GEN - Building the driver with LAC_HW_PRECOMPUTES is not supported in this version of the driver -

Title	**GEN - Building the driver with LAC_HW_PRECOMPUTES is not supported in this version of the driver**
Reference #	QATE-4015
Description	If the driver is built with the LAC_HW_PRECOMPUTES compiler option, the system may hang and/or crash.
Implication	The LAC_HW_PRECOMPUTES feature should not be used. Software precomputes, which are the default, must be used instead.
Resolution	Do not use the LAC_HW_PRECOMPUTES compiler option. This will not be fixed.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.22 QATE-6463 - GEN - icp_sal_userStart and icp_sal_userStartMultiProcess hang if they are called more than once in the same process -

Title	**GEN - icp_sal_userStart and icp_sal_userStartMultiProcess hang if they are called more than once in the same process**
Reference #	QATE-6463
Description	icp_sal_userStart and icp_sal_userStartMultiProcess hang if they are called more than once in the same process when no instances are left.
Implication	Caller to these functions can be blocked forever.
Resolution	This is resolved with the 0.9.2 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.23 QATE-3017 - CY - Zero length authentication requests affect the result of other processes using the authentication service -

Title	**CY - Zero length authentication requests affect the result of other processes using the authentication service**
Reference #	QATE-3017
Description	Zero length authentication requests affect the comparison result of other authentication requests using the same accelerator
Implication	An authentication check can report an incorrect negative value
Resolution	This is resolved with the 1.0.0 release.
Affected OS	Linux
Driver/Module	CPM FW

3.2.24 QATE-7909 - CY KPT - cpaCyKptRegisterKeyHandle() fails with error code 12 -

Title	**CY KPT - cpaCyKptRegisterKeyHandle() fails with error code 12**
Reference #	QATE-7909
Description	In stress conditions cpaCyKptRegisterKeyHandle fails with status = -1 and kptstatus = 12
Implication	Registration of KPT keys might fail.
Resolution	This was introduced in 1.0.1 release and is resolved with the 1.0.2 release.
Affected OS	Linux
Driver/Module	CPM FW

3.2.25 QATE-3650 - SRIOV - unbind of VFs to guests does not work properly when VF driver is loaded in the host -

Title	**SRIOV - unbind of VFs to guests does not work properly when VF driver is loaded in the host**
Reference #	QATE-3650
Description	We observed issues when detaching VFs from the host to a guest when the VF driver is loaded in the host.
Implication	Detaching VFs from a host to a guest as well as sharing VFs between host and guests might not work.
Resolution	Not a defect, test procedure has been updated.
Affected OS	Linux
Driver/Module	n/a

3.2.26 QATE-3259 - GEN - Package does not build on Centos 6.8 -

Title	**GEN - Package does not build on Centos 6.8**
Reference #	QATE-3259
Description	Due to changes in the Linux kernel, the software package may fail to compile on some newer Linux distributions, including CentOS 6.8.
Implication	The software package fails to compile.
Resolution	This is resolved with 1.0.2 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.27 QATE-8189 - CY - Key derivation function for PRF with SHA256 and 128 bytes secret causes unexpected results -

Title	**CY - Key derivation function for PRF with SHA256 and 128 bytes secret causes unexpected results**
Reference #	QATE-8189
Description	When performing a Key Derivation Function for TLS 1.2 for PRF, with a SHA256 hash, the accelerator hangs and reports a fatal error if the secret used is 128 bytes.
Implication	128 bytes secrets are not supported at this time. The accelerator might hang, report a fatal error, or produce incorrect results.
Resolution	This is resolved with 1.0.3 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.28 QATE-3563 - GEN - A Step: The driver can report Spurious Completion Abort Errors -

Title	**GEN - A Step: The driver can report Spurious Completion Abort Errors**
Reference #	QATE-3563
Description	The driver can report Spurious PCIe Completer Abort errors when a completion returns to the driver with Completer Abort status.
Implication	The end user may see spurious PCIe completion aborts errors coming from the driver. The driver will never generate completion abort errors under any other circumstances.
Resolution	This is resolved with Revision B silicon.
Affected OS	This is resolved with Revision B silicon.
Driver/Module	This is resolved with Revision B silicon.

3.2.29 QATE-3971 - DC - A Step: Static Compression failure when running static and dynamic in parallel -

Title	**DC - A Step: Static Compression failure when running static and dynamic in parallel**
Reference #	QATE-3971
Description	While running multiple static and dynamic compression threads in parallel for a few hours silent data loss can been seen.
Implication	When running static and dynamic compression in parallel over a long period of time it is possible to lose static data silently.
Resolution	This is resolved with Revision B silicon.
Affected OS	This is resolved with Revision B silicon.
Driver/Module	This is resolved with Revision B silicon.

3.2.30 QATE-3955 - DC - Compression operations involving payloads above 64K while using Compress and Verify functionality may fail -

Title	**DC - Compression operations involving payloads above 64K while using Compress and Verify functionality may fail**
Reference #	QATE-3955
Description	Compression operations using Compress and Verify functionality may fail with CpaDcReqStatus of CPA_DC_VERIFY_ERROR or CPA_DC_MCADECOMPERR. The issue is observed with sessions using payload sizes above 64K when Storage_Enabled = 1 in the device configuration file and the compression operations request that CpaDcOpData.mcaDecompressCheck = CPA_TRUE while calling cpaDcCompressData2() API
Implication	None
Resolution	This has been confirmed as a test code issue
Affected OS	Linux
Driver/Module	CPM IA - Sample Code

§

4.0 Frequently Asked Questions

4.1 I have an application called XYZ with the intent to use two cryptography instances from each of two chipset (PCH) devices in the system (a total of four instances). What would the configuration files look like?

In this case, the `NumberCyInstances` parameter should be set to 2 in the configuration file for each PCH device.

4.2 Should the Cy<n>Name parameter use unique values for <n> in each configuration file?

The `Cy<n>Name` parameter can be used in different configuration files without issue. In addition, the same `Cy<n>Name` name can be used in different domains within the same configuration file. The same rules apply to the `Dc<n>Name` parameter.

4.3 The firmware does not load. How can I fix this?

If the firmware does not load, verify that `udev` is available and running. On older systems (e.g., CentOS 6.5), verify that the kernel was built with `CONFIG_FW_LOADER=y`. On more recent systems (e.g., CentOS 7), `udev` is part of `systemd` and it is installed by default as part of the `systemd-udevd` service.

4.4 When I try to start the driver, I see errors (including kernel messages) that appear to be related to memory allocation. What can I do to avoid this?

When many instances are declared in the configuration file, it is possible to see these errors. The errors can typically be avoided by using the recommendations in the "Reducing Asymmetric Service Memory Usage" section of the *Intel® QuickAssist Technology Performance Optimization Guide*, by reducing the `NumConcurrentSymRequests` parameters in the configuration file, or by reducing the number of instances declared in the configuration file (see the "Acceleration Driver Configuration File" chapter in the chipset Programmer's Guide).

Another approach is to modify Linux* such that the value in `/proc/sys/vm/max_map_count` is increased (for example, to double the value). That value can be increased by modifying `/etc/sysctl.conf` to include the following line:

```
vm.max_map_count = <large_number_here>
```

Then reboot, and run `cat /proc/sys/vm/max_map_count` to verify that the value has been increased.

4.5 When trying to start the Intel® QuickAssist Technology driver, I see errors similar to one or more of the following:

Failed to send admin msg to accelerator

On systems that support PCIe* ECRC (PCIe transaction layer end-to-end CRC checking), such as Broadwell-based platforms, the root cause may be that ECRC is enabled in BIOS for the PCIe root ports. A proper fix will be for the BIOS to avoid enabling ECRC when devices are present that do not support ECRC or to disable ECRC by default in BIOS.

4.6 When loading the package modules, I see kernel log warnings related to signing of the modules. What do I need to do?

If certain kernel configuration flags are set (as some background, see `CONFIG_MODULE_SIG and CONFIG_MODULE_SIG_ALL)`, these messages may be returned. To avoid these warnings, consult the documentation for the applicable kernel configuration flags.

§