Intel® QuickAssist Technology (Intel® QAT) Software for Linux*

Release Notes

Package Version: QAT1.7.L.4.3.0-00033

September 2018

Document Number: 336211-008

Contents

Tables

Revision History

Released Revision History

Date	Revision	Description
September 2018	008	For software release QAT1.7.L.4.3.0-00033 Updated package number and checksum Updated New Features sub-section in Section 1.1 Updated Table 2 **New Open Issues:** QATE-29972, QATE-29974, QATE-30334, QATE-30497, QATE-30865, QATE-30880, QATE-30882, QATE-31295 **Newly Resolved Issues:** QATE-3982, QATE-14458, QATE-18691, QATE-20186, QATE-30340, QATE-30758, QATE-30785
June 2018	007	For software release QAT1.7.L.4.2.0-00012 Minor updates throughout for clarity Updated package number and checksum Updated Chapter 4. Added FAQ. **New Open Issues:** QATE-15136, QATE-17367, QATE-18691, QATE-20186, QATE-21561 **Newly Resolved Issues:** QATE-3039, QATE-3635, QATE-4051, QATE-11828, QATE-12793, QATE-14779, QATE-14870, QATE-14920, QATE-14953
April 2018	006	For software release 4.1.0-00022 Minor updates throughout for clarity Updated package number and checksum Updated Section 1.1 Updated Section 2.1 Updated Chapter 4. Added FAQ 7 **New Open Issues:** QATE-3350, QATE-7495, QATE-7919, QATE-12516, QATE-12793, QATE-14458, QATE-14706, QATE-14779, QATE-14870, QATE-14953, QATE-14920 **Newly Resolved Issues:** QATE-4111, QATE-5433, QATE-5520, QATE-5989, QATE-7393, QATE-7563, QATE-8109, QATE-8233, QATE-9234, QATE-9326, QATE-9483, QATE-10180, QATE-10780, QATE-11629, QATE-11790, QATE-12256, QATE-14171
January 2018	005	For software release 1.0.5-25
December 2017	004	For software release 1.0.5-14

Date	Revision	Description
August 2017	003	For software release 1.0.4-2
July 2017	002	**Newly Resolved Issues:** QATE-3955
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

Date	Revision	Description
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 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 (Intel® QAT).

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 2.3, Related Documentation).

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")
- Intel® Communications Chipset 8925 to 8955 Series

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® QuickAssist Technology Data Plane Cryptographic API (`cpa_cy_sym_dp.h`)
- Intel® QuickAssist Technology Data Plane Data Compression API (`cpa_dc_dp.h`)

The following feature is not currently supported:

- Dynamic instances
- KPT
- Batch and Pack in Compression service
- Stateful Compression is deprecated since this release

New Features

- Intel® QuickAssist APIs in kernel space (limited to Compression and Symmetric Cryptography)

- Compress and Verify and Recover (CnVnR) for DH895XCC chipset
- CnV statistics exposed in debugfs
- PF2VF comms performance improvements

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® Processor C3000 Product Family
- Intel® Xeon® D Processor Family
- Intel® Communications Chipset 8925 to 8955 Series

It has been validated against Yocto* for this product:

- Intel Atom® C3000 processor product family

Note: While the Intel® QuickAssist Accelerator software is validated on CentOS 7.x, it is expected that the current release will work without change on other Linux distributions and Kernels.

1.2.1 Version Numbering Scheme

The version numbering scheme is:

name.os.major.minor.maintenance-build

Where:

- *name* is “QAT1.7”
- *os* is the operating system: “L” for 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.4.3.0-00033.tar.gz

1.2.3 Licensing for Linux* Acceleration Software

The acceleration software is provided under the licenses listed in Table 4. Intel® QuickAssist Technology Software Specific Documentation. 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 only components	BSD	./quickassist/lookaside/access_layer/src/qat_direct ./quickassist/lookaside/access_layer/src/common/crypto/kpt ./quickassist/lookaside/access_layer/src/common/crypto/asym ./quickassist/utilities/osal/src/linux/user_space
Common User Space and Kernel Space Library	Dual BSD/ GPL v2	./quickassist/build_system ./quickassist/include ./quickassist/lookaside/ (except items in User Space only) ./quickassist/utilities/osal (except items in User Space only) ./quickassist/utilities/adf_ctl
Kernel space driver	GPL v2	./quickassist/qat/drivers
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
Calgary corpus and Canterbury corpus test files	Public domain	./quickassist/lookaside/access_layer/src/sample_code/performance/compression

NOTE: This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

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.

1.2.5 MD5 Checksum Information

The following table gives MD5 checksum information.

	Package	Checksum
Main Package	QAT1.7.L.4.3.0-00033.tar.gz	03e12bca9317ebda0a6b0c4821d20e91

1.3 Intel® QuickAssist Technology API Updates

Note: The Intel® 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*
- *Intel® QuickAssist Technology Data Compression API Reference Manual*

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 2.3, Related Documentation. If your field representative has created an account for you, support requests can be submitted via https://premier.intel.com.

§

2 Where to Find Current Software

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

2.1 Accessing Additional Content from My Intel

1. In a web browser, go to http://intel.com/myintel.
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 My Intel Business Applications & Tools, contact your Intel Field Sales Representative.
3. Enter your password in the **Password** box. Click **Submit**.
4. Under the **My Applications** heading, click on **Design Kits**
   a. Under the Processors, Boards, and Systems heading click on Processors and chipsets
   b. Search for the Code Name of the appropriate device.

      For the Intel® C62x Chipset PCH, enter the text **Purley** in the text box next to the Magnifying Glass

      For the Intel® Atom® C3000 Processor Product Family SoC, enter the text **Denverton NS**
   c. Click on the **View** button under the **Action** tab in the search results
   d. Click on the **Technical Library** tab

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.

2.3 Related Documentation

The following table 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

Document Name	Reference Number
Intel® QuickAssist Technology Performance Optimization Guide	330687
Using Intel® Virtualization Technology (Intel® VT) with Intel® QuickAssist Technology Application Note	330689

The following table 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

§

3 Intel® QuickAssist Technology (Intel® QAT) 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
- FW - Firmware
- PERF - Performance

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

3.1 Known Issues

3.1.1 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. The issue is not observed when 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

3.1.2 QATE-3350 - CY - skcipher, akcipher QAT implementations in kernel space do not support CRYPTO_TFM_REQ_MAY_BACKLOG

Title	CY - skcipher, akcipher QAT implementations in kernel space do not support CRYPTO_TFM_REQ_MAY_BACKLOG.
Reference #	QATE-3350
Description	Skcipher and akcipher implementations in the QAT driver are not capable of backlog requests.
Implication	Some kernel applications, e.g. dm-crypt, might report a kernel panic.
Resolution	None.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.1.3 QATE-4051 - GEN - Full device pass-through not available on KVM guests

Title	GEN - Full device pass-through not available on KVM guests.
Reference #	QATE-4051
Description	The new firmware authentication feature 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 issued. This causes firmware authentication to fail after the first firmware download. Full device pass-through might work in some conditions when using vfio and if the host kernel and the platform support it.
Implication	Direct mode feature not available on KVM guests for devices on full pass-through mode.
Resolution	Talk to your Intel® representative for more information.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.4 QATE-7495 - GEN - An incorrectly formatted request to QAT can hang the entire QAT endpoint

Title	GEN - An incorrectly formatted request to QAT can hang the entire QAT endpoint.
Reference #	QATE-7495
Description	This version of the QAT hardware does not perform request checking. It follows that a malicious application can submit requests that can bring down an entire QAT endpoint, which can impact other QAT jobs associated with the hardware. This presents a risk to be managed by the host and guest operating systems and other system policies. The exposure can extend to other guest operating systems or applications outside of the typical access boundary of the malicious guest or application.
Implication	All guest operating systems or other applications using QAT must be trusted, and/or other steps must be taken to ensure that an untrusted application or guest cannot submit incorrectly formatted requests.
Resolution	There is no workaround available. However, system policies (including limiting certain operating system permissions) can help to mitigate this issue.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.5 QATE-7919 - GEN - ICP_WITHOUT_THREAD not supported

Title	GEN - ICP_WITHOUT_THREAD not supported.
Reference #	QATE-7919
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	None.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.6 QATE-9383 - GEN - When StorageEnabled = 1, the QAT driver tries to register into the Linux Kernel Crypto framework

Title	**GEN - When StorageEnabled = 1, the QAT driver tries to register into the Linux Kernel Crypto framework.**
Reference #	QATE-9383
Description	When StorageEnabled = 1 is selected in the config file, the QAT driver tries to register itself into the Linux Kernel Crypto framework even if crypto operations are not available.
Implication	An error saying that akcipher selftest failed might be reported in the syslog.
Resolution	Ignore the errors reported in syslog.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.1.7 QATE-9545 - PERF - Performance drop with Scatter Gather Lists (SGLs) composed of flat buffers of 1460B

Title	**PERF - Performance drop with Scatter Gather Lists (SGLs) composed of flat buffers of 1460B.**
Reference #	QATE-9545
Description	Excluding DH895X devices, a moderate performance drop might be experienced when using SGLs if the size of each collected flat buffer is not a multiple of 1024 bytes.
Implication	Applications might not perform as expected.
Resolution	For performant applications, use flat buffers or SGLs with a single flat buffer, or ensure buffers within an SGL are 1024B aligned.
Affected OS	Linux
Driver/Module	CPM Firmware - Crypto

3.1.8 QATE-12516 - GEN - CpaInstanceInfo2.instID reports erroneous quotes

Title	GEN - CpaInstanceInfo2.instID reports erroneous quotes.
Reference #	QATE-12516

Description	The `CpaInstanceInfo2` structure returned from `cpaCyInstanceGetInfo2()` and `cpaDcInstanceGetInfo2()` shows that the field `"instID"` contains unneeded quotes. For example using default configuration files the following strings are printed when inspecting the `CpaInstanceInfo2` runtime structures:
	CY Instance zero shows:
	`CpaInstanceInfo2.instID = SSL_INT_0_"SSL0"`
	DC Instance zero shows:
	`CpaInstanceInfo2.instID = SSL_INT_0_"Dc0"`

Implication	If the application looks at the instID field, the comparison might need to include these erroneous quotes.
Resolution	None.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.9 QATE-15136 - Hang of asymmetric crypto engines might not be detected by heartbeat

Title	Hang of asymmetric crypto engines might not be detected by heartbeat.
Reference #	QATE-15136
Description	Heartbeat might not detect a hang of an asymmetric crypto engine.
Implication	Device might be reported as responsive even if one of the engine is hung.
Resolution	None.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.1.10 QATE-17367 - SRIOV - PF driver might report errors if device is reset

Title	SRIOV - PF driver might report errors if device is reset.
Reference #	QATE-17367
Description	If a manual or automatic device reset (FLR or SBR) is triggered as a result of an error (e.g. heartbeat failure, end fatal errors, etc.) on a system with QAT VFs enabled, the PF driver might report run time errors and might not recover.
Implication	Reset of the PF driver is not supported when VFs are enabled.
Resolution	None.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.11 QATE-21561 - CY - PkeServiceDisabled = 1 in user configuration file might cause a failure during driver initialization

Title	CY - PkeServiceDisabled = 1 in user configuration file might cause a failure during driver initialization.
Reference #	QATE-21561
Description	When PkeServiceDisabled is set to 1 in the configuration file the software (1) incorrectly registers PKE services with the Linux Kernel crypto infrastructure and (2) sets an incorrect mask for the asymmetric crypto capabilities.
Implication	The driver may fail to initialize, a software crash may occur, or failure will occur in PKE operations. Asym crypto capabilities are incorrectly reported to the user-space driver.
Resolution	In the configuration file GENERAL section, set ServicesEnabled to “dc” or “sym;dc”. This will prevent user-space asym crypto instances. In the KERNEL section, set NumberCyInstances to 0. This will prevent registering with the Linux Kernel crypto infrastructure.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.1.12 QATE-29972 - Gen - Compilation with Intel® ICC not supported

Title	Gen - Compilation with Intel® ICC not supported.
Reference #	QATE-29972
Description	When compiling the software package with the Intel® C Compiler (ICC), the compilation will fail.
Implication	Build with ICC compiler is not supported with this release.
Resolution	Talk to your Intel® representative for more information.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.13 QATE-29974 - Gen - Compilation on RHEL 6.9 not supported

Title	Gen - Compilation on RHEL 6.9 not supported.
Reference #	QATE-29974
Description	When compiling the software package on RHEL 6.9, the compilation will fail.
Implication	Build on RHEL 6.9 is not supported with this release.
Resolution	Talk to your Intel® representative for more information.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.14 QATE-30334 - SRIOV - QAT API in kernel space is not supported on host through virtual functions (VFs)

Title	SRIOV - QAT API in kernel space is not supported on host through virtual functions (VFs).
Reference #	QATE-30334
Description	When a kernel application tries to use the Intel® QAT API through an instance associated to a VF, DMAR protection errors are reported in the system logs.
Implication	It is not possible to access the QAT API in kernel space using VFs in the host.
Resolution	Do not use the QAT kernel API with VFs on the host. VFs on guest are supported.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.15 QATE-30497 - Gen - Huge pages are not supported on host when the iommu is on

Title	Gen - Huge pages are not supported on host when the iommu is on.
Reference #	QATE-30497
Description	When an application tries to use VFs on host with intel_iommu=on and huge pages enabled in USDM, DMAR protection errors are reported in the system log.
Implication	It is not possible to use huge pages with VFs on host.
Resolution	None.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.16 QATE-30865 - DC - Decompression hardware accelerator requires a minimal destination buffer size

Title	DC - Decompression hardware accelerator requires a minimal destination buffer size.
Reference #	QATE-30865
Description	If the destination buffer size is less than 258 bytes for a decompression operation, the hardware may return overflow without processing any data. This may occur if previous decompression operations indicates the next decompression operation will produce a 258 byte match, which corresponds to the largest possible representation of the lengths symbols in the deflate standard.
Implication	No uncompressed data is produced until enough output buffer is supplied.
Resolution	For decompression operations, the minimal destination buffer size should be 258 bytes.
Affected OS	Linux
Driver/Module	CPM HW – Data Decompression

3.1.17 QATE-30880 - Gen - Partial recovery when kernel space instances are in use

Title	Gen - Partial recovery when kernel space instances are in use.
Reference #	QATE-30880
Description	If a device error (uncorrectable error or heartbeat failure) occurs while an application in kernel space is using the QuickAssist API and if AutoResetOnError is set to 1 in the config file, the device will be stopped and reset but not restarted.
Implication	After the occurrence of an error, the device is stopped and instances associated to that device will not be available.
Resolution	The application should stop the instances and restart the device manually through the adf_ctl tool. The application is also required to re-allocate the instances.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.18 QATE-30882 - GEN - QuickAssist API in kernel space not validated on 32bit OSes

Title	GEN - QuickAssist API in kernel space not validated on 32bit OSes.
Reference #	QATE-30882
Description	The QuickAssist API in kernel space is not validated on 32 bit OSes.
Implication	When running the cpa sample code in kernel space on 32 bit systems, the test might report errors while allocating memory.
Resolution	None.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.19 QATE-31295 - GEN - Internal QAT Memory can be exposed

Title	GEN - Internal QAT Memory can be exposed.
Reference #	QATE-31295
Description	While performing penetration tests on QAT, the ability to read internal device memory was observed. This required root access on the platform. Processes running in virtual functions are not able to exploit this vulnerability.
Implication	Internal data structures may be visible to unauthorized users.
Resolution	Proper access controls remain a requirement for QAT enabled platforms.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2 Resolved Issues

3.2.1 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

3.2.2 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

3.2.3 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 - Crypto

3.2.4 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	Not a defect. Update System Time in target platform.
Affected OS	Linux
Driver/Module	Installer

3.2.5 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

3.2.6 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 make the system unusable.
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

3.2.7 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.
Resolution	This is resolved with the 0.8.0 release.
Affected OS	Linux
Driver/Module	CPM IA – Crypto

3.2.8 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

3.2.9 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

3.2.10 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	This is resolved with the 0.6.0 release.
Affected OS	Linux
Driver/Module	CPM FW - Data Compression

3.2.11 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	CPM IA - USDM

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	CPM IA - USDM

3.2.13 QATE-3563 - GEN - Lewisburg/Denverton: A Step: The driver can report Spurious Completion Abort Errors

Title	**GEN - Lewisburg/Denverton: 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 abort 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	Linux
Driver/Module	n/a

3.2.14 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	This is resolved with the 4.2.0 release.
Affected OS	Linux
Driver/Module	ADF - Kernel Mode

3.2.15 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

3.2.16 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

3.2.17 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

3.2.18 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

3.2.19 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

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

Title	**GEN - Lewisburg: Common Memory Driver incorrectly allocates memory of size between 2MB and 4MB.**
Reference #	QATE-3791
Description	This applies to LBG-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

3.2.21 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

3.2.22 QATE-3971 - DC - Lewisburg/Denverton: A Step: Static Compression failure when running static and dynamic in parallel

Title	DC - Lewisburg/Denverton: 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	Linux
Driver/Module	CPM IA - Data Compression

3.2.23 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

3.2.24 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.
Resolution	This is resolved with the 0.8.0 release.
Affected OS	Linux
Driver/Module	Test Code

3.2.25 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	This is resolved with the 4.3.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.26 QATE-3986 - GEN - The included memory driver impacts Traditional API sample code performance

Title	**GEN - The included memory driver impacts Traditional API sample code performance.**
Reference #	QATE-3986
Description	The included memory driver has a large impact on 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

3.2.27 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

3.2.28 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

3.2.29 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 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

3.2.30 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

3.2.31 QATE-4111 - DC - Engine timeout not handled correctly

Title	DC - 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.
Resolution	This is resolved with 4.1.0 release.
Affected OS	Linux
Driver/Module	CPM FW - Data Compression

3.2.32 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	This is resolved with the 4.1.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.33 QATE-5520 - DC – Stateful Dynamic compression might report a spurious CPA_DC_FATALERR

Title	DC – Stateful Dynamic compression might report a spurious CPA_DC_FATALERR.
Reference #	QATE-5520
Description	If the physical address (or io virtual address) of the PrivateMetaData of the compression context buffer has byte 0 set to 0x07 in the high part of address, the compression operation might fail with CPA_DC_FATALERR.
Implication	A spurious CPA_DC_FATALERR might be returned by the compression engine. After this error is reported, it is not possible to continue submitting jobs using the same session.
Resolution	This is resolved with the 4.1.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Data compression

3.2.34 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 QAT API results in an incorrect tag result.
Implication	Incorrect result when computing AES-CCM for zero length payloads.
Resolution	This is resolved with the 4.0.1 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.35 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

3.2.36 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 QAT API results in an incorrect tag result.
Implication	This is resolved with the 4.0.1 release.
Resolution	Set messageLenToHashInBytes to 0 in CpaCySymOpData when sending an AES-CCM zero-length request.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.37 QATE-7563 - SYM - Watchdog timer errors not reported to user callback

Title	SYM - Watchdog timer errors not reported to user callback.
Reference #	QATE-7563
Description	Watchdog errors are not reported to user callbacks for crypto operations.
Implication	If a watchdog timer expires, the user application is not notified.
Resolution	This is resolved with the 4.1.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.38 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 is resolved with the 1.0.2 release.
Affected OS	Linux
Driver/Module	CPM FW

3.2.39 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	This is resolved with the 4.0.1 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.40 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

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

Title	GEN - Installation of QAT Software on Yocto or Ubuntu image results in libraries not being placed in default system path.
Reference #	QATE-8233
Description	The shared library libqat_s.so may be installed somewhere other than the default directory.
Implication	Applications may fail to link to the libqat_s.so at run time. This has been observed with Yocto images and Ubuntu 15.x and 16.x.
Resolution	This is resolved with the 4.1.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.42 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	This is resolved with the 4.0.1 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.43 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	A kernel panic might happen at reboot if an application is using QAT.
Resolution	This is resolved with 1.0.5 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.44 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	This is resolved with the 4.0.1 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.45 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	This is resolved with the 4.1.0 release.
Affected OS	Linux
Driver/Module	ADF - Kernel Mode

3.2.46 QATE-10180 - DC - endOfLastBlock capability not properly reported by cpaDcQueryCapabilities

Title	DC - endOfLastBlock capability not properly reported by cpaDcQueryCapabilities.
Reference #	QATE-10180
Description	When querying the QAT driver using the function cpaDcQueryCapabilities, the API reports endOfLastBlock as CPA_FALSE even though this feature is supported by the hardware.
Implication	EndOfLastBlock is reported incorrectly to applications.
Resolution	This is resolved with the 4.0.1 release.
Affected OS	Linux
Driver/Module	CPM IA - Data compression

3.2.47 QATE-10780 - DC - Dynamic compression capability not properly reported by cpaDcQueryCapabilities

Title	DC - Dynamic compression capability not properly reported by cpaDcQueryCapabilities.
Reference #	QATE-10780
Description	When querying the QAT driver using the function cpaDcQueryCapabilities, the API reports dynamicHuffman as CPA_TRUE even though dynamic compression is not supported by this release.
Implication	It is possible to discover that dynamic compression is disabled only when calling cpaDcCompressData. This will impact the behavior of applications that query the device capabilities.
Resolution	This is resolved with the 4.0.1 release.
Affected OS	Linux
Driver/Module	CPM IA - Data compression

3.2.48 QATE-11629 - GEN - Module signature not supported by QAT installers

Title	GEN - Module signature not supported by QAT installers.
Reference #	QATE-11629
Description	The installer fails loading the QAT modules when Secure Boot is enabled in the platform. The QAT installer does not support signing kernel modules with a custom key.
Implication	QAT kernel modules should be signed manually in order to use UEFI Secure boot.
Resolution	This is resolved with the 4.0.1 release.
Affected OS	Linux
Driver/Module	Installer

3.2.49 QATE-11790 - CY - CPA_STATUS_FAIL reported for subsequent requests when a PKE request times out

Title	CY - CPA_STATUS_FAIL reported for subsequent requests when a PKE request times out.
Reference #	QATE-11790
Description	When an engine timeout is detected for the PKE service, subsequent requests might fail with the same error.
Implication	A reset will be required for future PKE requests to be ensured to succeed.
Resolution	This is resolved with the 4.1.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.50 QATE-11828 - GEN - Kernel panic observed in Intel® QAT driver for c62x included in kernels between v4.5 and v4.8

Title	GEN - Kernel panic observed in Intel® QAT driver for c62x included in kernels between v4.5 and v4.8
Reference #	QATE-11828
Description	When loading the Intel® QAT driver included in a kernel distribution, the platform might report a kernel panic.
Implication	When uninstalling the Intel® QAT driver, the Intel® QAT driver present in the distribution is re-loaded. This might cause a kernel panic.
Resolution	Not a defect in the current version of the software. Blacklist the QAT driver. Refer to instructions in the Getting Started Guide.
Affected OS	Linux with kernel version between 4.5 and 4.8
Driver/Module	ADF - Kernel Mode

3.2.51 QATE-11933 - GEN - rng operation in progress while unregistering qat aead implementation in the kernel

Title	**GEN - rng operation in progress while unregistering qat aead implementation in the kernel.**
Reference #	QATE-11933
Description	A crypto operation may be in progress when the aead implementation in the kernel is unregistered.
Implication	With a stress test which reboots a platform continuously, a kernel panic might be observed.
Resolution	This is resolved with 1.0.5 release.
Affected OS	Linux
Driver/Module	ADF - Kernel Module

3.2.52 QATE-12256 - VIRT - Device indices not handled correctly when a device is detached from the driver

Title	**VIRT - Device indices not handled correctly when a device is detached from the driver.**
Reference #	QATE-12256
Description	After detaching a device from the QAT driver, for example in preparation for passing a VF to a VM, qat_service might report inconsistent indices and BDFs.
Implication	qat_service might report inconsistent information after a device has been detached from the QAT driver.
Resolution	This is resolved with the 4.1.0 release.
Affected OS	Linux
Driver/Module	ADF - Kernel Mode

3.2.53 QATE-12793 - SYM - Algchain: chained crypto and hash requests for DES, 3DES and Kasumi might report an incorrect output digest

Title	**SYM - Algchain: chained crypto and hash requests for DES, 3DES and Kasumi might report an incorrect output digest.**
Reference #	QATE-12793
Description	When performing an algorithm chaining operation using DES CBC, 3DES CBC, Kasumi F8 as encryption algorithm and any hash algorithm, the result digest might be miscalculated.
Implication	Results digest from chained operations with DES CBC, 3DES CBC and Kasumi F8 might not be correct.
Resolution	This is resolved with the 4.2.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.54 QATE-14171 - Run time error if library is built with --enable-icp-dc-only

Title	Run time error if library is built with --enable-icp-dc-only.
Reference #	QATE-14171

Description	When the driver is built with --enable-icp-dc-only, the icp_sal_userStart() API might report a run time error similar to the following:
	`[error] SalCtrl_GetEnabledServices() - : Error parsing enabled services from ADF`
	`[error] SalCtrl_ServiceEventHandler() - : Failed to get enabled services`
	`ADF_UIO_PROXY err: adf_user_subsystemInit: Failed to initialise Subservice SAL`

Implication	"--enable-icp-dc-only" was not supported until the 4.1.0 release.
Resolution	This is resolved with the 4.1.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.55 QATE-14458 - GEN - Functional sample code fails to build when the package is built in dc-only mode

Title	**GEN - Functional sample code fails to build when the package is built in dc-only mode.**
Reference #	QATE-14458
Description	When the QAT package is built with option --enable-icp-dc-only, the functional sample codes fail to build reporting an error similar to the following: `make` `rm -vf *.o dc_stateless_sample` `cc -Wall -O1 -I/quickassist/include/ -I/quickassist/include/lac -I/quickassist/include/dc -l /quickassist/lookaside/access_layer/include -I/quickassist/lookaside/access_layer/src/sample_code/functional/include -I/quickassist/utilities/libusdm_drv// -DUSER_SPACE -DDO_CRYPTO -DWITH_UPSTREAM -DWITH_CMDRV ../../common/cpa_sample_utils.c cpa_dc_stateless_sample.c cpa_dc_sample_user.c -L/usr/Lib -L/build /build/libqat_s.so /quickassist/utilities/libusdm_drv//linux/build/linux_2.6/user_space/libusdm_drv.a -lpthread -lcrypto -ludev -o dc_stateless_sample` `/tmp/ccnX80N8.o: In function `sal_polling':` `cpa_sample_utils.c:(.text+0xb5): undefined reference to `icp_sal_CyPollInstance'` `/tmp/ccnX80N8.o: In function `sampleCyGetInstance':` `cpa_sample_utils.c:(.text+0x14e): undefined reference to `cpaCyGetNumInstances'` `cpa_sample_utils.c:(.text+0x169): undefined reference to `cpaCyGetInstances'` `/tmp/ccnX80N8.o: In function `sampleCyStartPolling':` `cpa_sample_utils.c:(.text+0x209): undefined reference to `cpaCyInstanceGetInfo2'` `collect2: error: ld returned 1 exit status` `/quickassist/lookaside/access_layer/src/sample_code/functional/dc/stateless_sample/../../common.mk:130: recipe for target 'default' failed` `make: *** [default] Error 1`
Implication	It is not possible to build the functional sample codes when the package is built in dc-only mode.
Resolution	This is resolved with the 4.3.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Sample code

3.2.56 QATE-14779 - CY - On SKUs with PKE service disabled, self-test fails when driver loads and watchdog timer errors might be reported

Title	**CY - On SKUs with PKE service disabled, self-test fails when driver loads and watchdog timer errors might be reported.**
Reference #	QATE-14779

Description	On SKUs with PKE disabled, the self-test provided by the linux kernel might fail with an error similar to the following
	`[ +1.167496] alg: akcipher: encrypt test failed. err -22`
	`[ +0.001260] alg: akcipher: test 1 failed for qat-rsa, err=-22`
	`[ +0.001478] alg: dh: generate public key test failed. err -22`
	`[ +0.001245] alg: dh: test failed on vector 1, err=-22`
	When running the cpa_sample_code, the PKE might fail with the following message:
	`[error] LacPke_MsgCallback() - : The slice hang error is detected on the MMP slice.`

Implication	No functional impact.
Resolution	The error can be ignored. Talk with your Intel® representative for more information.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.57 QATE-14870 - GEN - Library built with --enable-lac-hw-precomputes might report run time errors

Title	**GEN - Library built with --enable-lac-hw-precomputes might report run time errors.**
Reference #	QATE-14870
Description	The user space library might report run time errors (e.g. segmentation faults) if built with enable-lac-hw-precomputes.
Implication	lac-hw-precomputes configuration option is not supported in this release.
Resolution	This option has been removed since release 4.2.0.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.58 QATE-14920 - GEN - Library built with --enable-icp-trace might report run time errors

Title	GEN - Library built with --enable-icp-trace might report run time errors.
Reference #	QATE-14920
Description	The user space library might report run time errors (e.g. segmentation faults) if built with enable-icp-trace.
Implication	enable-icp-trace configuration option is not supported in this release.
Resolution	This has been confirmed to be a test issue.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.59 QATE-14953 - SRIOV - VF driver might report errors if device is reset

Title	SRIOV - VF driver might report errors if device is reset.
Reference #	QATE-14953
Description	If a manual or automatic device reset (FLR or SBR) is triggered as a result of an error (e.g. heartbeat failure, end fatal errors, etc.) on a system with QAT VFs enabled, the VF driver might report run time errors and might not recover.
Implication	Reset of the PF driver is not supported when VFs are enabled.
Resolution	None.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.60 QATE-18691 - DC – Incorrect consumed bytes reported during decompression

Title	DC – Incorrect consumed bytes reported during decompression.
Reference #	QATE-18691
Description	In some circumstances, the calculation of residue bits at the end of the decompression stream may be inaccurate.
Implication	For decompression requests where the last bfinal bit is 1, the number of bytes reported consumed may be incorrect. Also, for decompression requests where the last bfinal bit is 0, an extra byte of output may be emitted. This is not applicable to data compressed using the Intel® Communications Chipset 8925 to 8955 Series with bfinal=0 and bfinal=1. This is not applicable to data compressed by other accelerators covered by release 4.2.0 and prior with bfinal=1.
Resolution	This is resolved with the 4.3.0 release.
Affected OS	All
Driver/Module	CPM HW – Data Decompression

3.2.61 QATE-20186 - DC - endOfLastBlock not set in CpaDcRqResults during Stateful decompression with overflow of last chunk

Title	DC - endOfLastBlock not set in CpaDcRqResults during Stateful decompression with overflow of last chunk.
Reference #	QATE-20186
Description	When performing decompression operations in Stateful sessions, the application will not see the endOfLastBlock property set in CpaDcRqResults if the last request of the stream is zero byte long. This scenario may happen when the flush flag is set to CPA_DC_FLUSH_FINAL and overflow happens on the last packet of data to be decompressed.
Implication	The endOfLastBlock property is not set in the CpaDcRqResults structure. Consumed and produced fields in the CpaDcRqResults structure remain correct when the issue happens.
Resolution	This is resolved with the 4.3.0 release.
Affected OS	Linux
Driver/Module	CPM FW - Data Compression

3.2.62 QATE-30340 - GEN – Kernel panic during device power-off

Title	GEN – Kernel panic during device power-off.
Reference #	QATE-30340
Description	It is not possible to remove a QAT device driver with rmmod if there is a user space process using the device (attached to the driver). There is a reference counter preventing this from happening. However, If for any reason the kernel driver of a QAT device is removed while a user space process is running, the Kernel will crash. The user space library will send IOCTL to the Kernel space driver which will not be dealt because the Kernel driver is no longer available. This issue has been observed during a change of power mode state.
Implication	Dmesg will report a Kernel Oops. The user application may report a segfault and a reboot is required.
Resolution	This is resolved with the 4.3.0 release
Affected OS	Linux
Driver/Module	ADF - Kernel Mode

3.2.63 QATE-30758 - USDM - Suspected vulnerability in memory driver

Title	USDM - Suspected vulnerability in memory driver.
Reference #	QATE-30758
Description	The memory driver included in the software package can enable privilege escalation.
Implication	An unprivileged user process may be able to gain root privileges with a specialized kernel memory allocation attack.
Resolution	This is resolved with the 4.3.0 release.
Affected OS	Linux
Driver/Module	CPM IA - USDM

3.2.64 QATE-30785 - SYM – Request cookie not released in case of error

Title	SYM – Request cookie not released in case of error.
Reference #	QATE-30785
Description	If an error is encountered while processing a symmetric crypto request, the request cookie is not freed back to the cookie pool.
Resolution	This is resolved with the 4.3.0 release
Affected OS	Linux
Driver/Module	CPM IA - Crypto

§

4 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 (such as CentOS 6.5), verify that the kernel was built with CONFIG_FW_LOADER=y. On more recent systems (such as 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.

4.7 Why does QAT performance drop around buffer/packet sizes of 2kB?

Depending on the specifics of the particular algorithm and QAT API parameters, a relatively small decrease in performance may be observed for submission requests around a buffer/packet size of 2kB to 4kB. This is expected due to optimizations in the QAT software that can apply for requests of a certain size.

4.8 I am receiving failures or hangs when sending perform requests to the QAT API after a fresh boot or after hotplug events. How can these be resolved?

For the proper initialization, adf_ctl must be brought down and then back up (execute `adf_ctl down` followed by `adf_ctl up`) after a fresh boot. Various errors or hangs can occur if this is not done. Note that qat_service, if used, handles this. For hotplug events, remove the QAT modules and reinsert them before executing `adf_ctl down` and `adf_ctl up`.

§