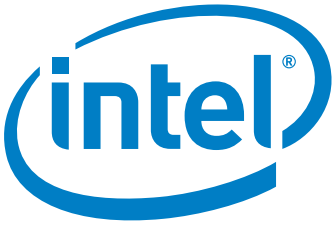

Intel® QuickAssist Technology Software for Linux*

Package Version: QAT1.5.L.1.13.0-19

Release Notes

November 2018

Document Number: 573029-012US

Contents

Tables

Revision History

Date	Revision	Description
November 2018	012	Added the following errata for the Intel® Communications Chipset 8900 to 8920 Series and/or Intel Atom® Processor C2000 Product Family for Communications Infrastructure: **Newly opened** • QATE-31832
May 2017	1.0	Created a new document from a previous document, with support for the Intel® Communications Chipset 8900 to 8920 Series and Intel Atom® Processor C2000 Product Family for Communications Infrastructure only. Added the following errata for the Intel® Communications Chipset 8900 to 8920 Series and/or Intel Atom® Processor C2000 Product Family for Communications Infrastructure: **Newly resolved** • IXA00398856 • IXA00398778 **Newly opened** • QATE-7741
May 2017	011	Added the following errata for the Intel® Communications Chipset 8900 to 8920 Series and/or Intel Atom® Processor C2000 Product Family for Communications Infrastructure: **Resolved** • QATE-7393
March 2016	010	Added the following errata for the Intel® Communications Chipset 8900 to 8920 Series and/or Intel Atom® Processor C2000 Product Family for Communications Infrastructure: **Resolved** • IXA00387832 • IXA00392516

§ §

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:

- Mux and QAT 1.6 drivers removed
- Support added for Intel Atom® Processor C2000 C0 silicon

For instructions on loading and running the release software, see the Getting Started Guide for your platform (see Section 2.3, "Related Documentation" on page 12).

Note: This software release is intended for platforms that contain:
- Intel® Communications Chipset 8900 to 8920 Series
- Intel Atom® Processor C2000 Product Family for Communications Infrastructure

Note: The Intel® QuickAssist Technology API for kernel space access is currently in the process of being deprecated in favor of making the Intel® QuickAssist Technology services available directly from the Linux kernel, including using the Linux Kernel Crypto framework. User space access is not affected.

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 of the software package are:

Table 1. Features of Platforms Using Intel® QuickAssist Technology

Feature/Limitation	Intel® Communications Chipset 8900 to 8920 Series	Intel Atom® Processor C2000 Product Family for Communications Infrastructure
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)	•	
Heartbeat Feature	•	•

1.2 Supported Operating Systems

The software in this release has been validated against the operating systems given in the following table on the Customer Reference Boards (CRBs) for the following products:

- Intel® Communications Chipset 8900 to 8920 Series
- Intel® Atom™ Processor C2000 Product Family for Communications Infrastructure

Note: While the Intel® QuickAssist Accelerator software is validated on Fedora* 16, CentOS 7, and Yocto* on the respective platforms, it should work without change on some other Linux* distributions and kernels.

Table 2. Operating System Support

Operating System	Intel® Communications Chipset 8900 to 8920 Series	Intel Atom® Processor C2000 Product Family for Communications Infrastructure
Fedora* 16 (32-bit and 64-bit)	•	
CentOS 7 (64-bit)	•	
Linux* (Yocto*)		•

1.2.1 Version Numbering Scheme

The version numbering scheme for all package levels is similar:

name.os.major.minor.maintenance-build

Where:

- *name* is the name of the package:
- *os* is the operating system, in all cases, "Linux*", denoted by 'L'
- *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.

Chipset or SoC	Package Version
Top-Level Package	QAT1.5.L.1.13.0-19.tar.gz

Note: For compatibility between QAT driver versions running on Host and Guest on a Virtualized Platform, see *Using Intel® Virtualization Technology (Intel® VT) with Intel® QuickAssist Technology Application Note* referenced in Table 4.

1.2.3 Licensing for Linux* Acceleration Software

The acceleration software is provided under a dual BSD/GPLv2 license with a few exceptions as listed in Table 3. When using or redistributing dual licensed components, you may do so under either license.

Table 3. Linux* Acceleration Software Licensing Files

Directory Name	License Used	Content Description
./quickassist/utilities/osal/thirdparty/openssl/include/*	OpenSSL	These are OpenSSL header files used for software- based hash pre-computes used with algorithm chaining. These hash pre-computes can be performed in hardware if needed. Refer to the Programmer's Guide for additional information.
./quickassist/lookaside/access_layer/src/sample_code/functional/sym/ssl_sample/*	GPLv2	Functional sample application illustrating the usage of Intel® QuickAssist Technology APIs in an ssl application.
./quickassist/utilities/osal/src/linux/kernel_space/*	GPLv2	Kernel space implementation of OS abstraction layer (OSAL). These functions are used only with the kernel space driver (icp_qa_al.ko). In user space, the OSAL layer source files are dual licensed.

1.2.4 BIOS/Firmware Version

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

It is important to update your platform so that it uses the latest available version of the BIOS/firmware that is available for that platform.

1.2.5 MD5 Checksum Information

The table below gives MD5 checksum information.

	Package	Checksum
Main Package	QAT1.5.L.1.13.0-19.tar.gz	960d89029ce75ce26c4d8f381a74b398

1.3 Intel® QuickAssist Technology Driver Information

To obtain driver information, use the command below corresponding to your chipset or SoC device:

- For Intel® Communications Chipset 8900 to 8920 Series:
  `cat /proc/icp_dh89xxcc_dev0/version`
- For Intel® Atom™ Processor C2000 Product Family for Communications Infrastructure:
  `cat /proc/icp_c2xxx_dev0/version`

The following is example output when using the Intel® Communications Chipset 8900 to 8920 Series. The output is similar for other devices.

```
[root@localhost build]# cat /proc/icp_dh89xxcc_dev0/version
+-------------------------------------------------+
| Hardware Software and API versions for device 0   |
+-------------------------------------------------+
 Hardware Version:             C1 SKU4
 Firmware Version:             1.12.1
 MMP Version:                  1.0.0
 Driver Version:               1.13.0
 QuickAssist API CY Version:   1.9
 QuickAssist API DC Version:   1.6
+-------------------------------------------------+
```

1.4 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 1.9
- Intel® QuickAssist Technology Data Compression API Reference Manual
  API Version 1.6
  (Not applicable to the Intel® Atom™ Processor C2000 Product Family for Communications Infrastructure since the Data Compression service is not supported on these SoCs.)

1.5 Patch Support

This release supports Intel-provided patch software for selected frameworks and applications such as OpenSSL and zlib. Supported patches are available on the 01.org website in the same location as the release software.

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

§ §

2.0 Where to Find Current Software

The software release and associated collateral can be found on the Intel's Open Source Technology Centre (https://01.org). See the access instructions following.

2.1 Accessing the Software

1. In a web browser, go to https://01.org/intel-quickassist-technology.
2. Scroll down to the RESOURCES section.

Note: The QAT1.5 driver can be found under the DH8900 to 8920 section and the the C2000 section.

3. Click on the `QAT1.5.L.<version>.tgz` link. The browser asks you if you want to download the file.
4. Save the file in the directory of your choice.
5. Unpack and install the software using the instructions in your platform's Getting Started Guide.

Note: The documentation related to the software is also available at the link in step 1.

For Intel® Atom™ Processor C2000 Product Family for Communications Infrastructure, additional documentation and software packages are available as described in the section following.

2.1.1 Accessing Additional Software for Intel Atom® Processor C2000 Product Family for Communications Infrastructure

1. In a web browser, go to www.ibl.intel.com.
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. Within the Design Kit Categories, under the **Platform & Solutions** heading, click **Embedded**.

   Under the **Performance Platforms** heading, click **Embedded Platform Code Named Rangeley for Communications and Embedded Applications**.

   a. For Intel Atom® Processor platform information, under the **Associated Collateral Lists** heading, click **Embedded Platforms: Rangeley/Avoton Platform - Platform**. This collateral list contains the product documentation listed in Table 7.

   b. For the Edisonville collateral, under the **Associated Collateral Lists** heading, click **Microserver Platform Code Named Edisonville - BIOS, Software and Tools**. This collateral list contains the product documentation listed in Table 9.

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

Table 4 lists Intel® QuickAssist Technology generic documentation.

Table 4. Intel® QuickAssist Technology 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
Intel® QuickAssist Technology Acceleration Software OS Porting Guide	330688
Using Intel® *Virtualization Technology (Intel® VT) with Intel® QuickAssist Technology Application Note*	330689

Table 5 lists Intel® Communications Chipset 8900 to 8920 Series specific documentation.

Table 5. Intel® Communications Chipset 8900 to 8920 Series Software Documentation

Document Name	Reference Number
Intel® Communications Chipset 8900 to 8920 Series Software for Linux* Getting Started Guide	330752
Intel® Communications Chipset 8900 to 8920 Series Software Programmer's Guide	330753
Intel® Communications Chipset 89xx Series FIPS Certification Guide	473819

Table 6, Table 7, Table 8 and Table 8 list Intel® Atom™ Processor C2000 Product Family for Communications Infrastructure specific documentation.

Table 6. Intel Atom® Processor C2000 Product Family for Communications Infrastructure Software Documentation

Document Name	Reference Number
Intel Atom® Processor C2000 Product Family for Communications Infrastructure for Linux* Getting Started Guide	330754
Intel Atom® Processor C2000 Product Family for Communications Infrastructure Programmer's Guide	330755
Intel Atom® Processor C2000 Product Family for Communications Infrastructure FIPS Certification Guide	523472

Table 7. Rangeley/Avoton Platform - Platform Documentation

Document Name	Reference Number
Mohon Peak Customer Reference Board CRB User's Guide	514980

Table 8. Intel® Data Plane Development Kit - Technical Documentation

Document Name	Reference Number
Intel® Data Plane Development Kit (Intel® DPDK) Release Notes Addendum for the Intel Atom® Processor C2000 Product Family for Communications Infrastructure	518900

Table 9. Microserver Platform Code Named Edisonville - BIOS, Software and Tools Documentation

Document Name	Reference Number
Mohon Peak CRB (Customer Reference Board) - BIOS Images	518736
Avoton/Rangeley SoC Linux Kernel Patch for ES0 and ES1 Silicon - Technical Advisory	518578
Intel® Avoton Ethernet – Edisonville and Rangeley PV - Networking Software Drivers	537330
Intel® Network Connections Tools, PV – LAN Software Tools	348742
Intel Atom® C2000 GbE eeproms	516867

§ §

3.0 Intel® Communications Chipset 8900 to 8920 Series and Intel Atom® Processor C2000 Product Family for Communications Infrastructure - Software Issues

Known and resolved issues are described in this section. Unless explicitly stated or noted, each issue relates to the Intel® Communications Chipset 8900 to 8920 Series and the Intel® Atom™ Processor C2000 Product Family for Communications Infrastructure.

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 chipset device stepping.

3.1 Known Issues for Intel® Communications Chipset 8900 to 8920 Series and Intel Atom® Processor C2000 Product Family for Communications Infrastructure

Note: Virtualization and Compression issues do not apply to Intel® Atom™ Processor C2000 Product Family for Communications Infrastructure.

The known issues in the current release are listed below.

Table 10. Summary of Known Issues

3.1.1 IXA00372157 - SRIOV: Shutdown of guest with inflight operations results in device hang -

Title	**SRIOV: Shutdown of guest with inflight operations results in device hang**
Reference #	IXA00372157
Description	A non graceful forced shutdown of a guest with inflight QA operations may result in a device hang. For example, issuing the command 'virsh destroy' for the guest.
Implication	Device hang. Device is unavailable for other guests and the host.
Resolution	Don't force shutdown, use a graceful shutdown, e.g. 'virsh shutdown' or shutdown from within the guest.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.2 IXA00385637 - DC: Zero-length compression requests are not supported when performing stateless data compression using multiple compress operations. -

Title	**DC: Zero-length compression requests are not supported when performing stateless data compression using multiple compress operations.**
Reference #	IXA00385637
Description	Zero-length compression requests are not supported when performing stateless data compression using multiple compress operations.
Implication	This feature is not available if the user performs zero-length compression requests.
Resolution	When performing stateless data compression using multiple compress operations, ensure that no requests with a zero length buffer size are submitted to the acceleration driver.
Affected OS	Linux
Driver/Module	CPM IA - Data Compression

3.1.3 IXA00386756 - GEN: Driver -12 error occurs when configuring for PF/VF concurrency on some platforms -

Title	**GEN: Driver -12 error occurs when configuring for PF/VF concurrency on some platforms**
Reference #	IXA00386756
Description	When starting the driver on some platforms with CentOS6.4, with a build and configuration that supports SR-IOV and with service instances allocated to the PF, -12 error occurs.
Implication	Running sample code fails and generates un-correctable error messages.
Resolution	Driver -12 error occurs when calling a kernel function which attaches the virtual function to IOMMU domain fails to find the page directory from the systems page table. This issue was observed on Stargo platform running CentOS 6.4. One alternative is to add iommu=pt to the kernel command line in the GRUB.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.4 QATE-7741 - PRF operation for Extended Master Secret gives incorrect result -

Title	**PRF operation for Extended Master Secret gives incorrect result**
Reference #	QATE-7741
Description	Extended Master Secret PRF Operations are not supported on the Intel Atom® Processor C2000 Product Family
Implication	OpenSSL 1.1.0 use Extended Master Secret PRF Operations by default rather than a Master Secret PRF Operation. TLS based applications using using OpenSSL 1.1.0 or later will not work using the OpenSSL QAT Engine.
Resolution	recompile the OpenSSL QAT Engine with PRF disabled
Affected OS	Linux
Driver/Module	CPM IA

3.1.5 QATE-8825 - F/W version does not match the release number -

Title	**F/W version does not match the release number**
Reference #	QATE-8825
Description	Firmware Version: for the 1.13.0 release is 1.12.1
Implication	None
Resolution	None
Affected OS	Linux
Driver/Module	CPM IA

3.1.6 QATE-31832 - USDM - Suspected vulnerability in memory driver -

Title	USDM - Suspected vulnerability in memory driver
Reference #	QATE-31832
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	Restrict account access on potentially affected machines.
Affected OS	Linux
Driver/Module	CPM IA - USDM

3.2 Resolved Issues for Intel® Communications Chipset 8900 to 8920 Series and Intel Atom® Processor C2000 Product Family for Communications Infrastructure

This section contains issues resolved since the following package versions:

- Intel® Communications Chipset 8900 to 8920 Series Software version 2.2.0.
- Intel Atom® Processor C2000 Product Family for Communications Infrastructure

Table 11. Summary of Resolved Issues

3.2.1 IXA00398856 - Gen: Application calls to QAT driver API "cpaCyKeyGenTls2" can return incorrect results -

Title	**Gen: Application calls to QAT driver API "cpaCyKeyGenTls2" can return incorrect results**
Reference #	IXA00398856
Description	Under high crypto load, in a multi-process environment, running both cipher operations and PRF key gen operations, input data to cipher operations in one process may appear as output data in another
Implication	Potential security issue
Resolution	Resolved in 1.7.3 & 1.13.0 Releases
Affected OS	Linux
Driver/Module	Acceleration Driver

3.2.2 IXA00398778 - CY: AES-GCM operation with zero length plain text results in an incorrect tag result -

Title	**CY: AES-GCM operation with zero length plain text results in an incorrect tag result**
Reference #	IXA00398778
Description	Sending an AES-GCM operation with zero length plain text to Cave Creek using the Quick Assist API results in an incorrect tag result
Implication	Potentially bad record errors and failing connections
Resolution	Resolved in 1.7.3 & 1.13.0 Releases
Affected OS	Linux
Driver/Module	Acceleration Driver

3.2.3 IXA00392717 - GEN: The driver fails to submit messages to the firmware causing no responses to be delivered and can cause shutdown issues on some application servers -

Title	**GEN: The driver fails to submit messages to the firmware causing no responses to be delivered and can cause shutdown issues on some application servers**
Reference #	IXA00392717
Description	The driver fails to submit messages to the firmware causing no responses to be delivered and can cause shutdown issues on some application servers. It can appear that the worker process is shutting down and the application server will not exit as it thinks this process is waiting on a response from the firmware that it will not get as no requests were actually sent to the firmware. This issue occurs when 2 or more processes are simultaneously trying to setup instances in the same bank.
Implication	If the previous value is overwritten by the latter one, then previous setting will be lost, which means the ring previously enabled will be disabled.
Resolution	Add a lock in quickassist/adf/transport/src/adf_HWarbiter.c around the WRITE_CSR_ARB_RINGSRVARBEN calls to make sure that the CSR written is successfully returned and to prevent two processes writing at the same time. Restarting the process can allow the process to send and receive messages successfully provided that a second process isn't also trying to simultaneously setup a instance on the same bank Addressed in Software Package
Affected OS	Linux
Driver/Module	ADF - Kernel Mode

3.2.4 IXA00168573 - CY: Algorithm chaining for AES-GCM can return an incorrect digest when using the Traditional API -

Title	**CY: Algorithm chaining for AES-GCM can return an incorrect digest when using the Traditional API**
Reference #	IXA00168573
Description	The problem occurs intermittently in a multi-threaded environment and does not affect the cipher text created.
Implication	Incorrect digest can be returned to the user.
Resolution	Addressed in the R1.1.0 Software Package
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.5 IXA00168788 - CY: Application crash when a user space application fails to initialize asymmetric crypto on IRQ mode only -

Title	**CY: Application crash when a user space application fails to initialize asymmetric crypto on IRQ mode only**
Reference #	IXA00168788
Description	When user space app fails to initialize PKE running in IRQ mode, it is possible that the application reports a segmentation fault. This issue is reproduceable when allocating and freeing dynamic instances again and again. The initialization will be done at each allocation. It can also be reproduced calling start/stop process APIs in user space again and again.
Implication	The driver will report a segmentation fault.
Resolution	Addressed in the R1.2 Software Package
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.6 IXA00168886 - DC: Decompression reports -10 soft error after processing stored block of size>=32KB -

Title	**DC: Decompression reports -10 soft error after processing stored block of size>=32KB**
Reference #	IXA00168886
Description	Stateful decompression of >=32K of specific compressed data can result in a -10 error status being returned to the application for a very specific set of compressed data.
Implication	If a user application receives the -10 error, it should split the data into packets of size <32K and resubmit the data.
Resolution	Addressed in the R1.3 Software Package
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.7 IXA00368704 - GEN: icp_sal_userStart hangs when there is no memory in SNB-EN slot -

Title	**GEN: icp_sal_userStart hangs when there is no memory in SNB-EN slot**
Reference #	IXA00368704
Description	When using the Shumway board with the default configuration, where SNB-EP is the host processor, but with only the SNB-EP banks populated with memory modules, the driver is not be able to bring up the acceleration device connected to the SNB-EN processor node. In kernel space, this results in an error logged in the system log. In user space, the icp_sal_userStart call hangs. This is due to an issue in the kernel that is tracked by this bugzilla entry: https://bugzilla.kernel.org/show_bug.cgi?id=42967
Implication	In kernel space, the instances set up on the second device are unavailable. In user space, the user is not able to execute the icp_sal_userStart function; consequently no instances are available.
Resolution	If a user wants to allocate instances on a particular CPU node, then it is required that this node will be populated with memory since the driver will call kmalloc_node (size, node). If no memory plugged into the memory controller for this node, then a crash will occur.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.8 IXA00369518 - DC B0 only: Only marginal increase in compression ratio at certain levels when stateful used and potential fatal error. -

Title	**DC B0 only: Only marginal increase in compression ratio at certain levels when stateful used and potential fatal error.**
Reference #	IXA00369518
Description	Due to current workarounds compression ratio during stateful compression at certain levels is affected. Recommended level is 32K L2 for best ratio gain. A fatal error may happen during stateful compression for level 2, 3, 5, 6, 8 or 9.
Implication	The compression ratio gain from using stateful compression will not be realised at the following levels: 32K History Window: L5,L6,L8,L9 8K History Window: L2,L3,L5,L6,L8,L9 The fatal error will return the error -13 in the compression callback.
Resolution	Resolved with C0 silicon.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.9 IXA00370156 - DC B0 Only - Decompression may hang if dynamic src data is incomplete. -

Title	**DC B0 Only - Decompression may hang if dynamic src data is incomplete.**
Reference #	IXA00370156
Description	The Hardware accelarator may hang during stateless decompression if the src data is incomplete and ends in the middle of a dynamic blocks trees.
Implication	The accelarator will hang and will be unresponsive.
Resolution	Resolved in C0 silicon.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.10 IXA00370174 - DC B0 Only - Decompression can hang if overflow occurs in the middle of a non-empty stored block > 8 Bytes -

Title	**DC B0 Only - Decompression can hang if overflow occurs in the middle of a non-empty stored block > 8 Bytes**
Reference #	IXA00370174
Description	There is a problem in the handling of overflow when it occurs in the middle of a non-empty stored block. Affects stateless and stateful decompression. This issue only affects B0 silicon.
Implication	The Compression slice can hang if an overflow occurs in the middle of a stored block that is greater than 8 bytes.
Resolution	A device reset is required when a hang is encountered. Resolved in C0, this issue only affects B0 silicon.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.11 IXA00371167 - DC B0 Only: Overflow may not be reported when incomplete data sent to the slice for decompression. -

Title	**DC B0 Only: Overflow may not be reported when incomplete data sent to the slice for decompression.**
Reference #	IXA00371167
Description	If overflow occurs during stateless decompression and the last byte is a data byte from a non-empty stored block then overflow will not be reported but the output from the Hardware Accelerator will be incomplete.
Implication	The output from the Hardware Accelerator is incomplete due to a possible overflow.
Resolution	There is currently no workaround for this issue in B0. The issue has been resolved in C0.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.12 IXA00371315 - DC B0 Only - Static output can be corrupted, Dynamic can hang on very rare occasions. -

Title	**DC B0 Only - Static output can be corrupted, Dynamic can hang on very rare occasions.**
Reference #	IXA00371315
Description	On very rare occasions, a hang can occur during stateless and stateful dynamic compression. The output from stateless and stateful static compression can also be corrupted.
Implication	A hang occurs and compression output can be corrupted.
Resolution	There is currently no workaround for this issue. This issue is resolved with chipset C0 silicon.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.13 IXA00371601 - DC B0 Only : Slice hangs during decompression of fixed/dynamic blocks without empty stored blocks padding to a byte -

Title	**DC B0 Only : Slice hangs during decompression of fixed/dynamic blocks without empty stored blocks padding to a byte**
Reference #	IXA00371601
Description	The driver incorrectly handles fixed/dynamic blocks without an empty stored block in between padding each block out to a byte boundary.
Implication	The driver can hang if it encounters this type of input. Affects both stateless and stateful decompression.
Resolution	No known workaround. This issue is resolved with chipset C0 silicon.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.14 IXA00371624 - SRIOV: Device hang on adf_ctl up when guest defines a service not enabled in host services -

Title	**SRIOV: Device hang on adf_ctl up when guest defines a service not enabled in host services**
Reference #	IXA00371624
Description	If the host only enables service "cy0" and guest attempts to define and use "cy1" then device hangs affecting both host and guest.
Implication	Device hang.
Resolution	All services to be used by guests should be enabled in the host configuration file.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.15 IXA00372583 - DC : Decompression can falsely detect soft error with certain input. -

Title	**DC : Decompression can falsely detect soft error with certain input.**
Reference #	IXA00372583
Description	During decompression certain dynamic trees can cause the decompression slice to falsely detect soft error. This situation occurs when, during the compression of a data set, the compressor generates a dynamic Huffman tree with the following characteristics: i) Exactly 256 symbols are used. ii) All the symbols have the same, or nearly the same frequency of occurrence. iii) All of the symbols are encoded to 8-bit codes. In this particular situation, during decompression, the decompressor does not process the tree correctly and returns an error that usually indicates a data error.
Implication	Soft error is encountered and decompression of stream cannot be completed.
Resolution	See the Stateful Compression - Dealing with Error Code CPA_DC_BAD_LITLEN_CODES (-7) section in the IntelÂ® Communications Chipset 89xx Series Software Programmerâ€™s Guide for more information
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.16 IXA00372698 - DC B0 Only - Decompression of stored blocks may cause CRC error -

Title	**DC B0 Only - Decompression of stored blocks may cause CRC error**
Reference #	IXA00372698
Description	During decompression of stored blocks an incorrect CRC/Adler may be returned.
Implication	During decompression of stored blocks an incorrect CRC/Adler may be returned.
Resolution	No workaround for this issue although CRC can be calculated in software.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.17 IXA00373407 - DC: Decompression service will continue to increment the consumed value for all data provided in the request after the final deflate block -

Title	**DC: Decompression service will continue to increment the consumed value for all data provided in the request after the final deflate block**
Reference #	IXA00373407
Description	The decompression service processes data up to and including a deflate block with a BFINAL bit set. If there is further data in the source buffer after the end of the BFINAL deflate block it will be not be processed. The behavior of the consumed byte counter (returned to the user via consumed value in CpaDcRqResults structure) cannot be predicted when the compression engine is fed with additional data after the end of deflate stream. Consecutive packets must be submitted as a Start of Packet. The acceleration slice does not understand Zlib or Gzip format therefore it is recommanded for the user not to submit the header nor the footer of the deflate stream to the compression slice.
Implication	If the source buffer provided to the decompression service contains data (e.g. a footer) after the BFINAL deflate block then the consumed value in CpaDcRqResults structure returned to the user is not correct. Subsequent packet sent to the slice will then fail to inflate.
Resolution	Addressed in the R1.5 Software Package
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.18 IXA00373795 - GEN: Segfault on exit of the performance sample user-space application with optimized wireless firmware -

Title	GEN: Segfault on exit of the performance sample user-space application with optimized wireless firmware
Reference #	IXA00373795
Description	When running the optimized wireless firmware, there is a segmentation fault on exit when operating in the following environment: - Wireless Firmware - 1024 byte packets or bigger - 4 instances (2 slices on 2 CPMs) - Traditional API
Implication	All tests run successfully, but there is a segmentation fault on exit, resulting in a memory leak.
Resolution	Addressed in the R1.0.1 Software Package
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.19 IXA00373970 - CY: wireless instance will hang when kill the process or use ctrl+c to exit the test -

Title	CY: wireless instance will hang when kill the process or use ctrl+c to exit the test
Reference #	IXA00373970
Description	While using the wireless firmware it is possible to cause a hang if the process is killed before it is finished. The hang is caused by the driver orphan thread handling not covering the wireless case correctly.
Implication	After the hang the device needs to be reset before it can process requests again.
Resolution	This is resolved in R1.7.2
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.20 IXA00378322 - CY: Performance drop for alg chain cipher then hash when append flag set -

Title	CY: Performance drop for alg chain cipher then hash when append flag set
Reference #	IXA00378322
Description	There is performance drop for Cipher-Hash operation when the digest is generated and inserted in to the destination buffer. The performance drop is observed comparing to Cipher-Hash operations when digest is generated and added to the separate buffer.
Implication	The algorithm remains functional. However, performance throughput levels for encrypt are reduced by 30-40%. Decrypt is unaffected.
Resolution	Addressed in the R1.0.1 Software Package
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.21 IXA00378522 - GEN : Cannot have different values of LimitDevAccess across device config files -

Title	**GEN : Cannot have different values of LimitDevAccess across device config files**
Reference #	IXA00378522
Description	Problems arise when LimitDevAccess is enabled in one config file, but disabled in another. The driver is not currently able to handle this mixed configuration.
Implication	Driver may not find the correct entries in the configuration file if this setting is different for each device in the system.
Resolution	Addressed in the R1.2.0 Software Package
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.22 IXA00378662 - DC: The upper word of the Adler checksum can be calculated incorrectly on very rare occasions -

Title	**DC: The upper word of the Adler checksum can be calculated incorrectly on very rare occasions**
Reference #	IXA00378662
Description	During decompression, because Adler32 is computed on four bytes at a time, the Compression slice incorrectly calculates the upper word of the Adler checksum. This situation occurs under the following conditions: i) The upper word of the current Adler calculation is in the vicinity of 0xFFF0. ii) The lower word of the current Adler calculation is in the vicinity of 0x7FFC. iii) The Adler32 computation for the next four bytes causes the upper word to exceed 0x2ffe0 before modulo arithmetic is performed. The modulo arithmetic is not done correctly in this case, causing an error in the checksum.
Implication	An erroneous checksum error is encountered after decompression is completed. There is no ability for the decompression solution to examine a checksum and determine that the problem occurred.
Resolution	Addressed in the R1.0.1 Software Package. A software workaround now takes care of this under the API.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.23 IXA00378701 - GEN : When slub_debug is defined in kernel space, seg fault when service is shutdown -

Title	**GEN : When slub_debug is defined in kernel space, seg fault when service is shutdown**
Reference #	IXA00378701
Description	When slub_debug is enabled at boot using the kernel parameters, the driver's memory allocation function can return non aligned memory thus crashing the driver during ring creation.
Implication	Cannot use slub-debug as a kernel parameter.
Resolution	Do not enable slub_debug at boot. Enable the relevant slub_debug parameters in the /sys/kernel/slub/* files once the system is up-and-running.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.24 IXA00378934 - CY: Crypto RSA segmentation fault while running performance tests in user space -

Title	**CY: Crypto RSA segmentation fault while running performance tests in user space**
Reference #	IXA00378934
Description	when running multiple threads performing primeTests on the same logical instance the application may run into the following error [error] cpaCyPrimeTest() - : Cannot get mem pool entry Segmentation fault (core dumped)
Implication	Performance test fails.
Resolution	Addressed in the R1.0.1 Software Package
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.25 IXA00378952 - GEN : Error over-riding a single logical Instance NumConcurrentRequest Value -

Title	**GEN : Error over-riding a single logical Instance NumConcurrentRequest Value**
Reference #	IXA00378952
Description	The V2 configuration file provides a general setting for the NumConcurrentRequests for each service: #Default values for number of concurrent requests*/ CyNumConcurrentSymRequests = 512 CyNumConcurrentAsymRequests = 64 DcNumConcurrentRequests = 512 The user should be able to override a single logical instance NumConcurrentRequest value using: CyXNumConcurrentAsymRequests = 512 where X= the instance number. However, the adf_ctl command or icp_sal_userStartMultiProcess function will report an error that the other instances are missing a corresponding CyXNumConcurrentAsymRequests parameter, but they should just use the default defined in the general section.
Implication	The user cannot overwrite settings for a single instance.
Resolution	If a user wants to overwrite a specific settings for an instance the entry for this needs to be put in a appropriate space in the instance definition. Configuration is processed from up - down and if the parser does not know about the specific configuration for a given instance, it will produce the default value. For example, when the user wants to overwrite the CyXNumConcurrentAsymRequests value for instance #1, it should be configured as above. # Crypto - User instance #1 Cy1Name = "SSL1" Cy1NumConcurrentAsymRequests = 128 Cy1IsPolled = 1 Cy1AcceleratorNumber = 1 # List of core affinities Cy1CoreAffinity = 1 In the below configuration, the specific value will not be taken into account and the default value will be generated. # Crypto - User instance #1 Cy1Name = "SSL1" Cy1IsPolled = 1 Cy1AcceleratorNumber = 1 # List of core affinities Cy1CoreAffinity = 1 Cy1NumConcurrentAsymRequests = 128
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.26 IXA00379409 - DC: cpaDcDecompressData reqs fail intermittantly on resubmit after CPA_STATUS_RETRY -

Title	**DC: cpaDcDecompressData reqs fail intermittantly on resubmit after CPA_STATUS_RETRY**
Reference #	IXA00379409
Description	If the user application resubmits both cpaDcCompressData or cpaDcDecompressData calls and if the driver returns status CPA_STATUS_RETRY, then: - The cpaDcCompressData call works fine on resubmits. - The cpaDcDecompressData call fails, not on every resubmit but just on some of them. It doesn't fail on the call itself but on the status returned within the results structure of the callback (the call is asynchronous). The error maybe any of the failure codes (-2, -13 etc).
Implication	The user application will see error codes (-2, -13 etc) and the data will not be decompressed.
Resolution	Addressed in the R1.1 Software Package
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.27 IXA00379630 - CY : NRBG cannot be used on 2nd crypto accelerator engine -

Title	**CY : NRBG cannot be used on 2nd crypto accelerator engine**
Reference #	IXA00379630
Description	The driver currently does not prevent the user from attempting to use NRBG functions on the second accelerator engine. There should be an error message to that effect, however, the driver behaviour in this situation is unpredictable.
Implication	Application may experience segmentation faults if it attempts to run NRBG on second accelerator engine.
Resolution	Only use Accelerators Engine number 0 on each accelerator. (or 0 and 2 when using V2 config file)
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.28 IXA00379858 - GEN : Heartbeat feature and error detection resets can cause GbE interfaces to go down -

Title	**GEN : Heartbeat feature and error detection resets can cause GbE interfaces to go down**
Reference #	IXA00379858
Description	When the acceleration driver detects either the firmware being unresponsive or other errors (detected through PCIe Advanced Error Reporting), it saves the PCIe state of the PCH and then performs a secondary bus reset of the IntelÂ® Communications Chipset 89xx Series device. Once the reset is complete, the driver restores the PCIe state of the PCH. At this point, the GbE interfaces have been reset and there were no saving/restoring of its PCIe state and there is no notification of this reset to the igb driver (if it was loaded and running). The GbE interfaces are no longer operational. Any network connections previously opened are now unresponsive.
Implication	The GbE interfaces will hang and will be unresponsive.
Resolution	The "heartbeat" feature and GbE Watchdog are described in the Getting Started Guide and the Programmer's Guide.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.29 IXA00380162 - CY: Kernel Opps Running qat_service shutdown before gige_watchdog_service stop -

Title	**CY: Kernel Opps Running qat_service shutdown before gige_watchdog_service stop**
Reference #	IXA00380162
Description	If the qat_service service is shutdown before the gige_watchdog_service the kernel will report an opps.
Implication	The kernel will report a kernel oops.
Resolution	Addressed in the R1.1 Software Package
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.30 IXA00380177 - DC: Decompressing files greater than 4 GB can result in an unreported error -

Title	**DC: Decompressing files greater than 4 GB can result in an unreported error**
Reference #	IXA00380177
Description	Decompressing files greater than 4 GB can result in an unreported error.
Implication	The compression job fails.
Resolution	Addressed in the R1.2 Software Package
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.31 IXA00380411 - CY: Deadlock for Partial Packets in user space -

Title	**CY: Deadlock for Partial Packets in user space**
Reference #	IXA00380411
Description	When creating multiple sessions all feeding partial packet requests to one instance, a deadlock can occur.
Implication	The driver will lockup.
Resolution	Addressed in the R1.2 Software Package.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.32 IXA00380578 - SRIOV: iommu_domain_alloc() crashes if IOMMU not enabled in the BIOS -

Title	**SRIOV: iommu_domain_alloc() crashes if IOMMU not enabled in the BIOS**
Reference #	IXA00380578
Description	It has been noticed that if in the BIOS, the fields: "VT-d" and "SRIOV Support" are disabled, the iommu_domain_alloc() function fails. The console reports: ============ Jan 15 08:45:44 localhost kernel: [148.892566] RIP [<ffffffff813b9029>] iommu_domain_alloc+0x3f/0x56 Jan 15 08:45:44 localhost kernel: [148.892680] RSP <ffff8802226d3e78> Jan 15 08:45:44 localhost kernel: [148.892750] CR2: 0000000000000000 Jan 15 08:45:44 localhost kernel: [148.892830] ---[end trace d612ff498c7f024b]--- Jan 15 08:45:45 localhost abrtd: Directory 'oops-2013-01-15-08:45:45-720-0' creation detected Jan 15 08:45:45 localhost abrt-dump-oops: Reported 1 kernel oopses to Abrt
Implication	iommu_domain_alloc() function fails and prevents the icp_qa_al from being insmoded correctly.

Title	SRIOV: iommu_domain_alloc() crashes if IOMMU not enabled in the BIOS
Resolution	Ensure that IOMMU is supported and enabled on the system.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.33 IXA00381020 - GEN: IA Driver - Osal - Error in osalIOMMUVirtToPhys function -

Title	GEN: IA Driver - Osal - Error in osalIOMMUVirtToPhys function
Reference #	IXA00381020
Description	While looking at the IOMMU support in the User Space side of the Osal Memory Driver: OsalUsrKrnProxy.c The function osalIOMMUVirtToPhys is called in the kernel space driver with an unmap call (DEV_MEM_IOC_IOMMUUNMAP) rather than a virt to phys call (DEV_MEM_IOC_IOMMUVTOP).
Implication	Memory deallocation will fail.
Resolution	Addressed in the R1.3 Software Package.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.34 IXA00381037 - DC: cpaDcRemoveSession return code check error. -

Title	DC: cpaDcRemoveSession return code check error.
Reference #	IXA00381037
Description	Issue 1: In the cpaDcRemoveSession() API, the spinlock was destroyed if the status to be return to the user was CPA_STATUS_RETRY. The spinlock should only be destroyed when the status is CPA_STATUS_SUCCESS. Issue 2: Before removing the session, it is necessary to verify the status of the rings to make sure these are empty. To do this, the API icp_adf_queueDataToSend() must be used. Originally, the verification was done using icp_adf_isRingEmpty() which was wrong.
Implication	Issue 1: If a retry occured then this could lead to timing problems. Issue 2: Ring may not be empty even so the driver thinks it is.
Resolution	Addressed in the R1.2 Software Package.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.35 IXA00381038 - DC: Potential memory leak in DC (Trad API) -

Title	DC: Potential memory leak in DC (Trad API)
Reference #	IXA00381038
Description	If a call to dcCreateRequest fails in dcCompDecompData, memory associated with the cookie is not freed.
Implication	This can lead to memory leaks when requests fail to be created.
Resolution	Addressed in the R1.2 Software Package.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.36 IXA00381173 - DC: Stateless Cumulative Checksum reports incorrect bytes consumed. -

Title	**DC: Stateless Cumulative Checksum reports incorrect bytes consumed.**
Reference #	IXA00381173
Description	The issue is present on stateless decompression and shows the consumed byte count being incorrect. The issue was seen with the following session settings: - Level 6 - Dynamic type - Deflate - AutoSelectBest enabled, - Adler32 checksum selected The test case used compressed a 512 block of data split into 2 scatter-gather lists. The compression operation worked fine but when trying to decompress the data, the expected consumed was different of what was produced during the compression operation. Switching the test to non-cumulative mode shows correct bytes consumed.
Implication	The decompressed data is invalid.
Resolution	Addressed in the R1.2 Software Package
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.37 IXA00381337 - SRIOV : Pass-through of IntelÂ® QuickAssist Technology PF and PCH GigE ports to a VM result in the GigE ports being non-responsive -

Title	**SRIOV : Pass-through of IntelÂ® QuickAssist Technology PF and PCH GigE ports to a VM result in the GigE ports being non-responsive**
Reference #	IXA00381337
Description	Pass-through of IntelÂ® QuickAssist Technology Physical Function (PF) and the PCH device GbE ports to a virtual machine result in GbE ports being nonresponsive after IntelÂ® QuickAssist Technology device initialization. IntelÂ® QuickAssist Technology Virtual Function (VF) pass-through with GbE port passthrough is not affected.
Implication	GigE ports are non-responsive.
Resolution	After IntelÂ® QuickAssist Technology device initialization, removing the igb module and re-inserting it allows both devices to work as normal.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.38 IXA00381487 - GEN: Dynamic instance allocation fails for 32-bit app on 64-bit OS -

Title	**GEN: Dynamic instance allocation fails for 32-bit app on 64-bit OS**
Reference #	IXA00381487
Description	The exisiting solution had an incompatible data structure size for 32 bit user space application running on 64-bit kernel space.
Implication	Dynamic instance would have issues running on 32 bit user space with 64 bit kernel space.
Resolution	Addressed in the R1.3 Software Package
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.39 IXA00381488 - DC: Errors not reported if session type is COMBINED and compression is dynamic -

Title	**DC: Errors not reported if session type is COMBINED and compression is dynamic**
Reference #	IXA00381488
Description	Errors from translation slice are ignored when the session direction is CPA_DC_DIR_COMBINED and huffType is CPA_DC_HT_FULL_DYNAMIC
Implication	If user's application configures the session so that the direction is combined and the compression type is dynamic then the user will not see any potential errors that could occur.
Resolution	Addressed in the R1.3 Software Package.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.40 IXA00381962 - CY: Need Param check in crypto APIs for CpaBoolean variables passed as pointers -

Title	**CY: Need Param check in crypto APIs for CpaBoolean variables passed as pointers**
Reference #	IXA00381962
Description	All the cpaCy APIs that take a boolean parameter as a pointer need to have this parameter check before being used.
Implication	If the user decides to pass a null pointer to this parameter, the driver will report a segmentation fault.
Resolution	Parameter check added to verify that the pointer address being passed is not NULL.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.41 IXA00381968 - GEN: Typo in CONFIG_PCI(E)AER -

Title	**GEN: Typo in CONFIG_PCI(E)AER**
Reference #	IXA00381968
Description	The linux kernel has the flag CONFIG_PCIEAER set when Advanced Error Reporting is supported. Making a typo on this #define prevents the code within CONFIG_PCIEAER section not to be compiled.
Implication	Advanced Error Reporting feature is not available.
Resolution	Addressed in the R1.3 Software Package.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.42 IXA00382154 - GEN: Error in ring handling when using interrupts in user space -

Title	**GEN: Error in ring handling when using interrupts in user space**
Reference #	IXA00382154
Description	When using interrupt mode with a user space QA application, the response ring head is not always updated during response processing and so the interrupt condition persists. The root of the issue is that a previous SW optimization coalesces response ring head updates. This optimization should not be applied when the response ring is in interrupt mode.
Implication	The fact that interrupts are re-enabled causes a the same interrupt to fire again multiple times. This leads to significant drop in system performance.
Resolution	In the API adf_ring_ioc_create_handle(): The ring_handle.min_resps_per_head_write is now set 0 in interrupt mode. Thi sprevents the interrupt from firing again. The ring_handle.min_resps_per_head_write = ring_data->minRespsPerHeadWrite in polling mode
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.43 IXA00382531 - CY: more cleanup code in osal_init is needed -

Title	**CY: more cleanup code in osal_init is needed**
Reference #	IXA00382531
Description	If function calls with osal_init fail, then the driver will not be unregistered and the crypto interface may not be uninitialized.
Implication	This can lead to memory leaks in the kernel space.
Resolution	The driver now calls the API unregister_mem_device_driver() if the osalCryptoInterfaceInit() fails. If the API osalIOMMUInit() fails, the driver now calls both unregister_mem_device_driver() and osalCryptoInterfaceExit() APIs.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.44 IXA00382601 - DC: Stateful compression operation can return false fatal error. -

Title	**DC: Stateful compression operation can return false fatal error.**
Reference #	IXA00382601
Description	Under heavy load when simultaneously running compression and cryptography operations, certain stateful compression operations on very particular input can return a false fatal error (error code -13).
Implication	The compression job for the session will fail and will need to be resubmitted.
Resolution	The firmware has been modified to remove the Fatal error reporting. Addressed in the R1.3.1 software package.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.45 IXA00382623 - DRAM Read in counter mode does not consume desc read signal correctly -

Title	**DRAM Read in counter mode does not consume desc read signal correctly**
Reference #	IXA00382623
Description	During a DRAM read operation of the scatter gather list, the decision to read the next flat buffer is made at the wrong time. This issue is visible when using dynamic compression and under a heavy load of traffic. Timing / IO latency all play a role when it comes to the manifestation of this issue. The problem shows when the compression firmware does not read the entire SGL. Dynamic compression or cases where the compression length in the request parameters is less than the length of the SRC flat buffer (inside the SGL) will be the main culprits. During DRAM read counter mode when not all of the flat buffers are populated with data we want to read we set the num of buffers in local memory to zero and the current buffer size to the dram read counter. The problem occurs because the decision to read the next flat buffer is made *before* the decision to modify these values. For correct operation it needs to happen after.
Implication	Consequences: - In the static compression scenario, we may end up with compressed data but not the ones that we expect - In the case of dynamic comnpression scenario, we may get slice error or history corruption.
Resolution	Firmware has been modified in 1.4 release so the decision to read the next flat buffer is made after the number of flat buffer is set to 0 in local memory.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.46 IXA00382936 - CY: When starting an application that uses a large number (>16) of processes, a timeout error may occur -

Title	**CY: When starting an application that uses a large number (>16) of processes, a timeout error may occur**
Reference #	IXA00382936
Description	The issue was observed using the openssl speed application patched with libcrypto* (OpenSSL*) Sample Patch for Intel(R) QuickAssist Technology. Libcrypto's openssl speed test uses multiple processes (instead of multiple threads) to measure performance. Each process has access to one crypto instance. When running a test with 16 or 32 processes, the test can fail from time to time reporting: [error] SalCtrl_AdfServicesStartedCheck() - : Sal Ctrl failed to start in given time [error] do_userStart() - : Failed to start services can't use that engine
Implication	Time-out errors may occur when starting a user space application when a large number (>16) of processes is used.
Resolution	This is resolved in QAT1.5 R1.5.0
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.47 IXA00382998 - CY: Driver lockup with RC4 cipher when hit ring full -

Title	CY: Driver lockup with RC4 cipher when hit ring full
Reference #	IXA00382998
Description	When doing decryption with the RC4 cipher which has lots of threads submitting decrypt requests to a single instance, eventually one thread hits ring full (CPA_STATUS_RETRY). That thread then resubmits the same request but no response will be received.
Implication	For multi threaded operations, if the ring is already full and a re-submitted request receives a CPA_STATUS_RETRY then this request will not receive a response. The bug is in function LacSymQueue_RequestSend() in file lookaside/access_layer/src/common/crypto/sym/lac_sym_queue.c. Before putting the request on the ring, the function assigns: - pSessionDesc->nonBlockingOpsInProgress = CPA_FALSE; This indicates that a blocking operation is in flight. The function then attempts to write the request to the ring. If the write to the ring is not successful, then the function fails to restore the nonBlockingOpsInProgress flag. Subsequent requests are queued in the session's queue, waiting for a pending operation which does not exist.
Resolution	A check has been added in lac_sym_queue.c so that if the icp_adf_transPutMsg fails then the nonBlockingOpsInProgress is reset to CPA_TRUE to prevent the driver from waiting for a request to be process that has not been sent down to the firmware.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.48 IXA00382999 - CY: Hit ring full when number of threads << ring size -

Title	CY: Hit ring full when number of threads << ring size
Reference #	IXA00382999
Description	The ring reports full for an invalid reason.
Implication	The driver returns frequent CPA_STATUS_RETRY errors, requests are being resubmitted and performance decreases.
Resolution	The number of inflight messages is decremented just before the callback is invoked rather than updating the number of inflight messages after all the callback have been called.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.49 IXA00383390 - DC: High rates of simultaneous crypto and (de)compression operations may cause in correct compression output and write an incorrect amount of data into the output buffer -

Title	**DC: High rates of simultaneous crypto and (de)compression operations may cause in correct compression output and write an incorrect amount of data into the output buffer**
Reference #	IXA00383390
Description	An incorrect compression output may be generated during some compression / decompression operations. This soft error indicates that an incorrect amount of data was written to the (de)compression output buffer in memory. It may not write enough data to memory or it may write too much data to memory. The issue is most likely to occur when running both symmetric cryptographic operations and compression/decompression operations at the same time with high request/traffic rates. When the issue occurs, the cryptographic operations are unaffected. The issue is highly unlikely to occur when running only compression/decompression operations (i.e. without concurrent cryptographic operations). The issue will not occur when running cryptographic operations alone. In the scenario where not enough data is written to the output buffer, data is missing and hence the compressed/decompressed data is incomplete and hence invalid.
Implication	If too little data is written the compressed/decompressed data is incomplete and hence invalid. If too much data is written the compressed/decompressed data is valid but additional data is present in the output buffer. If the issue occurs, only Intel(r) QuickAssist accelerator compression/decompression operations are affected.
Resolution	Resubmit the failed Intel(r) QuickAssist accelerator compression/decompression request. This issue will be resolved in a future release of the acceleration driver.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.50 IXA00383454 - CY: Performance Sample Code digestAppend setting is not optimal -

Title	**CY: Performance Sample Code digestAppend setting is not optimal**
Reference #	IXA00383454
Description	The performance sample code for the symmetric and symmetric data plan code is setting the digestAppend flag to true. This does not yeild the best performance results. In general, the difference is small. However, for 2048 bytes buffers and greater the digestAppend=true follows an unoptimized data path and therefore, the impact is more significant. Files affected: cpa_sample_code_sym_perf.c cpa_sample_code_sum_perf_dp.c
Implication	Symmetric AlgChain performance does not maximize the silicon potential.
Resolution	The cpa_sample_code_sym_perf.c and cpa_sample_code_sum_perf_dp.c files contain the following functions: setupAlgChainTest and setupAlgChainDpTest. These two functions call setupSymmetricTest and setupSymmetricDpTest. The last parameter is the digestAppend flag, this needs to be set to CPA_FALSE. Note: Changing this may result in some alg-chain combinations having invalid parameters.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.51 IXA00383572 - DC: Report overflow from XLT when byte count mismatch detected -

Title	DC: Report overflow from XLT when byte count mismatch detected
Reference #	IXA00383572
Description	During a dynamic compression operation, the translator slice will not report an overflow error if the dynamic output is greater than the static output.
Implication	Compressed data returned to the user will be correct. The user will not be aware that XLT has overflowed if the dynamic output is greater than the static output after the re-submit. This has no effect on the user application.
Resolution	This issue is resolved in R1.5.0
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.52 IXA00384087 - GEN: icp_adf_check_device() API fails to detect when firmware hang. -

Title	GEN: icp_adf_check_device() API fails to detect when firmware hang.
Reference #	IXA00384087
Description	Under certain circumstances, an ME hang due to the read() function called from the icp_adf_check_device() API may go undetected. The function checks for the return value however, it is also required to verify the content of the file.
Implication	if the read function does not fail, it may be able to read /proc/icp_dh89xxcc_dev0/qat0 that could be zero length and therefore it would not catch a firmware hang issue.
Resolution	To resolve this issue, we now read the content of the file /proc/icp_dh89xxcc_dev0/qat0 to make sure that the content is valid.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.53 IXA00384581 - GEN: The NumberConcurrent options in the configuration file will be overwritten to be half of the requested value. -

Title	GEN: The NumberConcurrent options in the configuration file will be overwritten to be half of the requested value.
Reference #	IXA00384581
Description	The configuration file holds the number of concurrent requests for Sym, Asym and DC. The Number of Concurrent request is user configurable, but this user value is divided by 2.
Implication	Mismatch between the number of concurrent requests defined by the user in the configuration file and the number of concurrent requests used by the driver.
Resolution	This issue is resolved in the R1.5.0.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.54 IXA00384651 - CY: When ICP_WITHOUT_THREAD is defined, enabling poll mode will cause a core dump -

Title	**CY: When ICP_WITHOUT_THREAD is defined, enabling poll mode will cause a core dump**
Reference #	IXA00384651
Description	If defining ICP_WITHOUT_THREAD and setting the instance poll mode to be 0, then a QAT Driver core dump occurs.
Implication	The QAT Driver will core dump.
Resolution	This issue is resolved in R1.5.0
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.55 IXA00384930 - CY: Issue with data plane GCM operations when using the acceleration driver -

Title	**CY: Issue with data plane GCM operations when using the acceleration driver**
Reference #	IXA00384930
Description	According to API documentation, values for hashStartSrcOffsetInBytes and messageLenToHashInBytes are not required and are intended for internal purposes for GCM operations. If these values are not set, GCM operations do not work with the data plane APIs. The driver is responsible for setting these values and this is not currently being done. This issue does not occur with the traditional GCM operations.
Implication	Crypto operations fail.
Resolution	This issue is resolved in R1.5.0
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.56 IXA00384933 - GEN: Unnecessary extra interrupts generated in user mode -

Title	**GEN: Unnecessary extra interrupts generated in user mode**
Reference #	IXA00384933
Description	In user space, if configured to use interrupts, more interrupts are generated than are necessary. In /proc/interrupts, the number of interrupts shown is greater than the number of responses received. (Corresponds to IXA00384677 on QAT1.6)
Implication	Unnecessary interrupt processing wastes CPU cycles.
Resolution	Addressed in the R1.5 Software Package
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.57 IXA00384934 - CY: Silent drop of messages -

Title	CY: Silent drop of messages
Reference #	IXA00384934
Description	When Crypto partials are in flight, messages can get queued in the driver so they are processed sequentially, that is, the next request is not put on the ring to the firmware until the response from the previous request has been received. If the response ring has been polled 10,000 times and the response is not received, the queued requests are silently dropped. (Corresponds to IXA00384681 on QAT1.6)
Implication	An application could remain waiting indefinitely for a response and not be aware that the request has been dropped.
Resolution	This issue is resolved in R1.5.0
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.58 IXA00385456 - GEN: Response ring processing is unnecessarily restricting request submissions -

Title	GEN: Response ring processing is unnecessarily restricting request submissions
Reference #	IXA00385456
Description	The inflight count for ring messages is not updated until after all callbacks handled together have been completed. This can lead to the ring pair reporting full, even though there is space available on the rings. The inflight counter should be decremented as soon as the response msg has been picked up in the response ring rather than after a burst of callbacks have been completed.
Implication	A RETRY response can be received when trying to put a message in the ring even though space is available.
Resolution	This issue is resolved in R1.5.0
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.59 IXA00385555 - GEN: The driver does not completely enable all error correction and detection (ECC and Parity) in the accelerator -

Title	GEN: The driver does not completely enable all error correction and detection (ECC and Parity) in the accelerator
Reference #	IXA00385555
Description	All previously released IntelÂ® QuickAssist Technology drivers do not have some of the ECC error correction and some of the parity detection logic enabled in the accelerator.
Implication	In the logic that does not have ECC error correction enabled, a single bit error will be treated as an uncorrectable error. For the limited memory that has parity detection disabled, a parity error will NOT be treated as uncorrectable. Uncorrectable errors may cause the accelerator to halt.
Resolution	This issue is resolved in R1.5.0
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.60 IXA00385634 - DC: Static decompression can falsely detect soft error with certain input. -

Title	DC: Static decompression can falsely detect soft error with certain input.
Reference #	IXA00385634
Description	It was noticed that the fix for IXA00372583 was not enabled if the session type was set to CPA_DC_HT_STATIC. The fix for this IXA was verifying if the session was set to Dynamic. This was wrong as a the fix for IXA00372583 needs to be applied in all types of sessions (dynamic /static).
Implication	As a consequence it could have happened that the IXA00372583 workaround would not be applied. The user would have seen a (-7) error code reporting a soft error.
Resolution	This issue is resolved in R1.5.0
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.61 IXA00385765 - GEN: Heartbeat test fails - platform does not recover and requires a reset -

Title	GEN: Heartbeat test fails - platform does not recover and requires a reset
Reference #	IXA00385765
Description	Under a heavy CPU load, it has been observed that when the driver is compiled with ICP_HEARTBEAT set, the Acceleration Engines may not restart when the firmware hangs. We've observed that the Acceleration Engines are stopped (as they should be) but won't be restarted.
Implication	As a consequence, the DH89xxCC device will halt as the firmware will not be reloaded
Resolution	This issue is resolved in R1.5.0
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.62 IXA00385873 - GEN: free_page usage issues -

Title	GEN: free_page usage issues
Reference #	IXA00385873
Description	OSAL API userMemFreePage() uses free_page() while userMemFreeAllPagePid() and userMemFreeAllPagePid() use __free_page. __free_page() and free_page() are defined as follow: #define __free_page(page) __free_pages((page), 0) #define free_page(addr) free_pages((addr),0) There is also some inconsistency in the parameter being passed to the free_page() calls.
Implication	No known effect to date.
Resolution	This is resolved with the R1.5 release.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.63 IXA00386021 - GEN: Higher than expected CPU cycles used in some low-traffic cases -

Title	GEN: Higher than expected CPU cycles used in some low-traffic cases
Reference #	IXA00386021
Description	This applies to CY / DC acceleration in user-space using polled rings. In response message handling, the CSR write coalescing logic results in the ring head CSR being written more frequently than necessary. This occurs in some low-traffic cases and results in an increased CPU cycle count for those cases. In high traffic cases, many responses are processed by the same poll and the ring head CSR writes are coalesced. In the case where only a small number of responses are processed by a poll, the head CSR is written in each poll, as the CSR write coalescing doesnâ€™t kick in.
Implication	More CPU cycles are used.
Resolution	This is resolved with the R1.5 release.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.64 IXA00386067 - SRIOV Issue in running sample code sign of life twice in Guest and Host parallel -

Title	SRIOV Issue in running sample code sign of life twice in Guest and Host parallel
Reference #	IXA00386067
Description	On the second run of sample code on Host and Guest in parallel the following error was observed: [error] LacPke_VerifyMmpLib() - : Error in LAC initialisation. Compiled firmware version (0x972DED54) does not match loaded firmware version (0x00000000)
Implication	A second run of sample_code may fail after the first run has passed.
Resolution	This is fixed in QAT1.5 v1.5.0
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.65 IXA00386090 - GEN: QAT R1.3.7 driver cause Linux kernel crash -

Title	GEN: QAT R1.3.7 driver cause Linux kernel crash
Reference #	IXA00386090
Description	After powering on/off the system and run performance test, it is possible to see a Linux kernel crash. If the response to a administration message sent from the QAT driver (using QatCtrl_SendAdminMsg()) takes longer that 300 Jiffies to respond then the semaphore associated with the message is deleted. The response arriving after 300 Jiffies will try to modify the semaphore and cause a kernel crash. Here is QAT call flow, 1.icp_adf_check_device->PROC file system/proc/icp_dh89xxcc_dev/??/qat0, then QatCtrl_Debug->QatCtrl_FWCountGet->QatCtrl_SendAdminMsg->QatCtrl_AdminMsgSendSync 2.QatCtrl_AdminMsgSendSync put msg in RING, then call LacSync_WaitForCallback to wait for response. If after 300 jiffies, No response, then it will remove the pSyncCallbackCookie->sid 3.The call back function QatCtrl_AdminSyncCb() will POST pSyncCallbackCookie->sid
Implication	Linux kernel will crash and will require a reboot
Resolution	This is resolved with the R1.5 release.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.66 IXA00386143 - GEN: Add support for Linux Kernels greater than 3.10 in order to enable debug information in proc file system -

Title	**GEN: Add support for Linux Kernels greater than 3.10 in order to enable debug information in proc file system**
Reference #	IXA00386143
Description	The following commands were not supported when QAT driver was running on system with a kernel greater than 3.10 cat /proc/icp_dh89xxcc_dev0/qat0 cat /proc/ icp_dh89xxcc_dev0/cfg_debug cat /proc/icp_dh895xcc_dev0/et_ring_ctrl/bank_9/ring_0 The entries were created but the files in the /proc were empty.
Implication	It is impossible to debug or to understand the driver behavior
Resolution	This is resolved in R1.6.0.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.67 IXA00386517 - GEN: Issue in SRIOV Physical passthrough for 2 devices to single VM -

Title	**GEN: Issue in SRIOV Physical passthrough for 2 devices to single VM**
Reference #	IXA00386517
Description	When two physical function are assigned to a single VM then the sample code fails to run in kernel space.
Implication	The firmware hangs and the following message is displayed. cat /proc/ icp_dh89xxcc_dev1/qat0 ERROR: Qat is not responding. Please restart the device
Resolution	The root cause for this issue is that Qemu does not pass the interrupt request from guest to host. Upgrade Qemu to 1.2.0 to reolve this issue.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.68 IXA00386714 - CY: digestIsAppended option is not fully supported for Hash-Only operations -

Title	**CY: digestIsAppended option is not fully supported for Hash-Only operations**
Reference #	IXA00386714
Description	Digest Verify is not currently supported for appended digest in Hash-Only operations (i.e. within the CpaCySymSessionSetupData structure, if symOperation=CPA_CY_SYM_OP_HASH then setting both verifyDigest=TRUE AND digestIsAppended=TRUE is not supported).
Implication	Incorrect digest verify result.
Resolution	When DigestVerify is required do not append the digest, pass it in in a separate buffer.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.69 IXA00387310 - DC: Error with stateful compression with CPA_DC_DIR_COMBINED -

Title	**DC: Error with stateful compression with CPA_DC_DIR_COMBINED**
Reference #	IXA00387310
Description	When the session direction is CPA_DC_DIR_COMBINED and the session is STATEFUL, the first decompression operation after at least one compression operation may not succeed.
Implication	Errors may be generated at the start of a session if mixing compression and decompression.
Resolution	This is resolved in R1.7.0.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.70 IXA00387481 - GEN Large value for CyXNumConcurrentXXXRequests causes system crash if not enough memory -

Title	**GEN Large value for CyXNumConcurrentXXXRequests causes system crash if not enough memory**
Reference #	IXA00387481
Description	On a CRB with 4G memory setting the following in the configuration file crashes the CRB: Cy0NumConcurrentSymRequests = 65336 Cy0NumConcurrentAsymRequests = 65336 The driver comes up ok in a system with 16G memory. The crash occurs while parsing the configuration file. Linux runs out of memory and starts closing services, rendering the board unusable. If the driver is installed with the installer then rebooting the board does not resolve the issue as the file is parsed again on reboot.
Implication	The system is unusable if there's not enough memory on board to satisfy memory requirements driven by NumConcurrentRequests configuration.
Resolution	Recovery can be achieved by rebooting in recovery mode and either reducing NumConcurrentRequest values in the configuration files or installing more memory on the CRB.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.71 IXA00387832 - DC: Dynamic Compression may lead to data loss -

Title	**DC: Dynamic Compression may lead to data loss**
Reference #	IXA00387832
Description	When using dynamic compression to compress data, it is possible to get an error (CPA_DC_BAD_DIST_CODE) during decompression. No notification is available upon compression. The compressed data cannot be decompressed.
Implication	Data compressed with the dynamic compression feature may not decompress to obtain the original data.
Resolution	This is resolved in R1.11
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.72 IXA00388387 - SRIOV: ./adf_ctl up fails to bring up the DH89xxCC device in a Guest with QATmux environment -

Title	**SRIOV: ./adf_ctl up fails to bring up the DH89xxCC device in a Guest with QATmux environment**
Reference #	IXA00388387
Description	With both DH89xxCC and DH895xCC devices in a Guest and the QATmux pkg installed the DH89xxcc device fails to come up, with following error: ./adf_ctl icp_dev1 u Processing file: /etc/dh89xxccvf_qa_dev0.conf ADF_CONFIG_CTL err: adf_read_config_file: ERROR: cy(n) is incompatible with dh895xcc device: use 'cy' in /etc/dh89xxccvf_qa_dev0.conf
Implication	In a QATmux environment on a Guest, DH89xxCC devices cannot be used.
Resolution	This is resolved in R2.2.0
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.73 IXA00388394 - CY: Incorrect Cy Session Ctx size returned by Dynamic API when hashMode = NESTED -

Title	**CY: Incorrect Cy Session Ctx size returned by Dynamic API when hashMode = NESTED**
Reference #	IXA00388394
Description	If using cpaCySymSessionCtxGetDynamicSize API the value returned when hashMode= CPA_CY_SYM_HASH_MODE_NESTED is less than the memory size required. If the exact memory size returned is then provided to the session the driver will access memory outside of this address space. This could result in a driver crash or in the driver overwriting data belonging to another application.
Implication	QAT Driver could access memory outside of area provided, with undefined results.
Resolution	This is resolved in R1.7.0
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.74 IXA00388840 - CY: cpaCySymRemoveSession fails in DP API if other active Session sharing ring -

Title	**CY: cpaCySymRemoveSession fails in DP API if other active Session sharing ring**
Reference #	IXA00388840
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 in R2.3.1
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.75 IXA00388846 - GEN: Warning in log in sync mode operation -

Title	GEN: Warning in log in sync mode operation
Reference #	IXA00388846
Description	When calling the QA API using synchronous mode (Callback = NULL) in some cases the following msg is seen in the logs LacSync_DestroySyncCookie() - : Attempting to destroy an incomplete sync cookie This has no impact on functionality. However it does indicate a memory leak of about 20 bytes. This has been seen if running cpa_sample_code RSA tests, but may also occur in other cases.
Implication	None
Resolution	This is resolved in R1.7.2.
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.76 IXA00389842 - CY: CPA_CY_SYM_HASH_AES_GMAC algorithm capability is not added -

Title	CY: CPA_CY_SYM_HASH_AES_GMAC algorithm capability is not added
Reference #	IXA00389842
Description	For a customer using strict capability checking using the API cpaCySymQueryCapabilities they will not be able to perform a AES128-GCM HMAC-AES-GMAC operation
Implication	For a customer using strict capability checking using the API cpaCySymQueryCapabilities they will not be able to perform a AES128-GCM HMAC-AES-GMAC operation
Resolution	This is resolved in R2.5.0
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.77 IXA00392516 - GEN: Inflight counter being overwritten for ring pairs in adjacent banks -

Title	GEN: Inflight counter being overwritten for ring pairs in adjacent banks
Reference #	IXA00392516
Description	Max number of inflight requests can be reached without actually filling the ring. The inflight count for each ring pair in bank 0 is at the same address as the corresponding ring-pair in bank 1. Similarly, bank 2 counters overlap with bank 3 counters, etc. This affects both Data Plane and Traditional APIs in user space, not in kernel space on both QAT1.5 and QAT1.6.
Implication	CPA_STATUS_RETRY's will be received on both input rings for both instances even though there is room on the ring.
Resolution	This is resolved in R1.11
Affected OS	Linux
Driver/Module	Feature - Acceleration Driver

3.2.78 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

4.0 Frequently Asked Questions

The following codes that prefix each title identify which platform each FAQ applies to:

- A - Intel® Communications Chipset 8900 to 8920 Series
- B - Intel Atom® Processor C2000 Product Family for Communications Infrastructure

4.1 [A] I am seeing PCIe Bus Errors when executing the sample code (cpa_sample_code).

These errors could be caused by one of the following:

- incorrect PCIe De-emphasis setting.
  Use -3.5dB for trace lengths < 11” and -6dB for trace lengths > 11”. The Root Complex that the EndPoint is connected to needs to request the -3.5 de-emphasis when training in Gen2.
- Max Payload Size mismatch between the Root Port and each EndPoint.

One way to test this is to transmit traffic and see if this works. If this does, then perform loopback test. If this fails, then one of the above is the likely source.

4.2 [A] I am using Intel® Communications Chipset 8900 to 8920 Series (PCH) SKU2, but the acceleration service does not start correctly. How do I resolve this?

Verify that your configuration file does not declare an index for `AcceleratorNumber` or `ExecutionEngine` that is greater than that which your device supports. If you are running the sample code, copy `dh89xxcc_qa_dev0_single_accel.conf` from `quickassist/config` to `/etc/dh89xxcc_qa_dev0.conf`, restart the acceleration service, and try again.

4.3 [A] 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.

4.4 [A] 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.

4.5 [A] Since the SSL data and the KERNEL sections in the configuration files for two Intel® Communications Chipset 8900 to 8920 Series (PCH) devices are identical, it is unclear how an application is able to use instances from more than one device. How does the application know which device each instance maps to?

The application can use the `cpaCyInstanceGetInfo2()` function to query which physical device an instance handle belongs to. For any application domain defined in the configuration files ([KERNEL], [SSL] and so on), a call to `cpaCyGetNumInstances()` returns the number of instances defined for that domain across all configuration files. A subsequent call to cpaCyGetInstances() can be used to obtain the instance handles. The `cpaCyInstanceGetInfo2()` function can then be used with an instance handle to identify which device a given instance maps to.

4.6 [A] Given the configuration below, what do the cpaCyGetNumInstances() and cpaCyGetInstances() functions return for each application and kernel domain?

Given this configuration:
- Application ABC: defines two crypto instances on dev0 only
- Application DEF: defines two crypto instances on dev1 only
- Application XYZ: defines four crypto instances (two on dev0, two on dev1)
- KERNEL: defines eight ctypto instances (four on dev0, four on dev1)

The `cpaCyGetNumInstances()` function returns the following:
- Application ABC: 2
- Application DEF: 2
- Application XYZ: 4
- KERNEL application domain: 8

The `cpaCyGetInstances()` function returns the following:
- Application ABC: two handles on dev0
- Application DEF: two handles on dev1
- Application XYZ: four handles (two on dev0 and two on dev1 in the order given)
- KERNEL application domain: 8 handles (four on dev0, four on dev1 in the order given)

Note: The order in the last two permutations is important.

4.7 [A] How can an application use instances from more than one Intel® Communications Chipset 8900 to 8920 Series (PCH) device when the [SSL] and [KERNEL] sections in both configuration files provided in the software package are identical?

An application must call `cpaCyInstanceGetInfo2()` on each handle returned from cpaCyGetHandles() and sort them by device. The `cpaCyInstanceGetInfo2()` function allows the user to query which physical device an instance handle belongs to. To expand somewhat, for any application domain defined in the configuration files ([KERNEL], [SSL] and so on), a call to `cpaCyGetNumInstances()` returns the number of instances defined for that domain across all configuration files, a subsequent call to `cpaCyGetInstances()` would obtain these instance handles.

4.8 [A] Driver compiles correctly, but acceleration service fails to start. How do I fix this?

A typical reason why the acceleration service does not start is that the `intel_iommu=off` kernel boot option was not specified, as required and documented in the *Getting Started Guide*.

The following errors are seen in this scenario:

```
[error] QatCtrl_InitMsgSendSync() - : Callback timed out
[error] QatCtrl_SendInitMsg() - : Failed to send Init msg 0 to AE 0
[error] SalCtrl_QatStart() - : Sending SET_AE_INFO msg Failed

[error] SalCtrl_QatEventStart() - : Failed to start all qat instances
icp_qa_al err: adf_subsystemStart: Failed to start subservice QAT
icp_qa_al err: adf_do_init: adf_subsystemInit error, stopping and shutting down
```

4.9 [A, B] The firmware does not load. How can I fix this?

If the firmware does not load, verify that `udev` is available and running, and verify that the kernel was built with `CONFIG_FW_LOADER=y`.

4.10 [A, B] 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.

4.11 [A] I'm seeing errors related to Uncorrectable Push/Pull Misc Errors

If you are attempting to access acceleration services on the host system when SR-IOV Host Acceleration software is installed, you may see errors like the following:

```
    icp_qa_al err: adf_dh895xcc_adf_isr)handleUncoInterrupt: Uncorrectable Push/
Pull Misc Error
    memory status: No errors occured - Transaction Id 0x0 - Error type reserved
    Bus Operation Type Push - Id 0x80000
    Reset needed for device: icp_dev0
```

This error would normally indicate a problem with hardware, but it may be addressed with a simple configuration file update. Ensure the following parameters are included in the configuration file in the [GENERAL] section:

- `SRIOV_Enabled = 1`
- `PF_bundle_offset = 5`

After making these updates, restart the acceleration software.

4.12 When trying to start the qat_service, it fails, and I see the following error message: "icp_qa_al: module verification failed: signature and/or required key missing - tainting kernel". What is the issue?

There are at least two possible scenarios that can lead to this case:

1. The BIOS/UEFI is preventing the module from loading. In this case, look for a BIOS/UEFI option to allow the module to load (e.g., disable Secure Boot).
2. On newer kernels, the upstreamed Intel QuickAssist Technology kernel modules conflict with those from the separate installation package. The newer qat_service scripts will rmmod these automatically when the service is started, but if an older qat_service script is used, or if `adf_ctl` is used, some additional logic is required to **rmmod** the conflicting upstreamed modules or to prevent them from loading.

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

- "QatCtrl_SendSyncMsg() - : AE response received to admin cmd 1, Fail status: 1”
- “SalCtrl_QatStart_dh895x() - : Sending TRNG_ENABLE msg Failed”
- "QAT: Could not find a device on node X”

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.