



Apollo Lake Platform - Intel® Trusted Execution Engine (Intel® TXE) 3.0 Firmware

HF Release Notes

Rev 3.0.11.1131

Intel Confidential

October 2016



You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at Intel.com, or from the OEM or retailer.

No computer system can be absolutely secure. Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at intel.com, or from the OEM or retailer.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or visit www.intel.com/design/literature.htm.

Intel and the Intel logo, are trademarks of Intel Corporation in the U.S. and/or other countries. *Other names and brands may be claimed as the property of others.

© 2016 Intel Corporation. All rights reserved.



Revision History

Revision Number	Description	Revision Date
3.0.11.1131	HF 3.0.11.1131	October 2016
3.0.10.1129	PV Release – RS1	September 2016
3.0.2.1108	HF2	August 2016
3.0.1.1107	HF1	July 2016
3.0.1.1105	PV / RS1-Beta Release	July 2016
3.0.0.1078	Beta Release	Februray 2016
3.0.0.1058	Alpha Release	December 2015



Contents

1	Fixed Issues	5
2	Intel® TXE Known Bugs	6
3	Intel® TXE Tools Known Bugs	7
4	Implemented RCRs	8



1 Fixed Issues

The following table lists all fixed issues in this release.

Issue #	Title	Description/ Affected component
1208817310	TXEInfo and TXEManuf response time is very slow under SHELL	Description: TXEInfo and TXEManuf tools' time response is longer than expected in UEFI shell. Affected component: Intel® TXE FW
1804341420	Intel® TXE response to GUC timeout causes PAVP tear down	Description: Intel® TXE response to GUC timeout causes tear down in PAVP when performing HDMI hotplug in PR3 playback. Affected component: Intel® TXE FW
1304657871	Intel® TXE FW performs a CSE reset & host reboots when running S3 stress with CPU & GPU load.	Description: When running stress (S0->S3->S0) with GPU loading (playing HD movie) & CPU loading for around a 100 iterations, Intel® TXE FW performs CSE reset & host reboot. Affected component: Intel® TXE FW



2 Intel® TXE Known Bugs

The following table lists known issues in this release.

Issue #	Title	Description/ Affected component
1304677586	Updateimage check MKHI returns an error when using an image without OEM hash key	Description: Capsule upgrade or downgrade fail when using an image without OEM hash key Affected component: Intel® TXE FW



3 Intel® TXE Tools Known Bugs

The following table lists all known issues related to TXE tools in this release.

Issue #	Title	Description/ Affected component
1304679385	EOM is set even if user choose "no" after closemnf	Description: EOM bit is set even if the user choose not to set it when executing closemnf. Affected component: Intel® TXE SW Tools
1405111690	EFI FPT commands WriteToken & EraseToken throw unexpected exception.	Description: When run from Intel® FPT, WriteToken & EraseToken return an error message and a failure message (even though successfully erased) respectively. Affected component: Intel® TXE SW Tools
1405151259	When trying to flash full SPI image with Intel® FPT, a warning is thrown regarding the file size difference.	Description: A warning is thrown when trying to flash a full size image using Intel® FPT tool. "Warning: Not all of the file data will be written to flash because the file is longer than the flash area to be written to!" Affected component: Intel® TXE SW Tools
1304675894	Intel® TXE region appears as not present when using Intel® FPT	Description: Intel® FPT tool should print the Intel® TXE region addresses instead of showing it as not present. Affected component: Intel® TXE SW Tools
1504329370	No correct part id to build the debug token	Description: Missing part id from DnX and an incorrect format in the part id dumped by fpt, hence, cannot build a valid debug token for injection. Affected component: Intel® TXE SW Tools



4 *Implemented RCRs*

N/A