



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

HF1 Release Notes

Rev 3.0.1.1107

Intel Confidential

July 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
3.0.0.1058	<ul style="list-style-type: none">Alpha Release	December 2015
3.0.0.1078	<ul style="list-style-type: none">Beta Release	Februray 2016
3.0.1.1105	<ul style="list-style-type: none">PV / RS1-Beta Release	July 2016
3.0.1.1107	<ul style="list-style-type: none">HF1	July 2016



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/ Impact
1604206242	System hang after re-flashing the IFWI firmware using FPT	Description: This issue will cause system hang and display black screen after flashing the IFWI FW via FPT followed by global reset via host only. Affected component: TXE FW and TXE Tools Impact: Manufacturing Status: Fixed in TXE FW and tools Recommendation: Due to nature of issue of FPT flashing, to avoid system hang after the immediate global reset, avoid flashing with FPT when system is running TXE FW 3.0.0.1.1105 or earlier. If you do desire to flash with FPT while target system is running 3.0.0.1.1105 or earlier TXE FW, then the system hang can be resolved by applying G3 then powering up the target.
1405091552	FPT fails to read "Disable Data Clear" in Post EOM	Description: FPT throws Error 57: Failed getting variable "Disable Data Clear" value in Post EOM Steps to Reproduce: 1) Perform EOM using "fpt -closemfn" 2) Read VARS using "fpt -r all" Expected: All the VARS are retrieved. Actual: Error 57: Failed getting variable "Disable Data Clear" value Affected component: TXE Tools. FPT Impact: Manufacturing Status: Fixed in TXE tools



2 *Intel® TXE Known Bugs*

NA

§



3 Intel® TXE Tools Known Bugs

The following table lists all known issues in this release.

Issue #	Title	Description/ Affected Component
1405067496	FPT -cfggen needs to remove unsupported features for OEMSKURule and FeatureShipState CVARS from config file	Description: FPT -cfggen generated config file should remove AMT and NFC related info. Affected component: INTEL TXE SW Tool
1304504977	EOM file is being written even when -closemnf operation fails.	Description: -closemnf operation fails, but nevertheless EOM flow is executed on the next boot. Affected component: INTEL TXE SW Tool
1304523381	After EOM unable to write any token (no write access) via DnX flow using PFT.	Description: DnX flow (via PFT) does not have write access after closeManuf for debugging a first boot scenario (when data is cleared) with token. After first boot, token can be pushed via DnX or via FPT. Affected component: INTEL TXE SW Tool
1208423519	FPT displays incorrect value for BootGuard in CFGGEN file	Description: Fpt -r BootGuard" prints the correct value "Profile 0 - Legacy" as the output, whereas cfggen output prints it as "Pr" only Affected component: INTEL TXE SW Tools

§



4 *Implemented RCRs*

NA

§