

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

## PV Release Notes

***Rev 3.0.1.1105***

**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 |
|---|---|---|
| 3.0.1.1105 | PV 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 ..... 9

3 Intel® TXE Tools Known Bugs ..... 10

4 Implemented RCRs ..... 11


§



# 1 Fixed Issues

The following table lists all fixed issues in this release.

| Issue # | Title | Description/ Affected component |
|---|---|---|
| 1304543790 | CSE FW PRTC driver must poll for write-in-progress after issuing a write command. | **Description:** HW taking time to complete a write cycle caused a delay in FW clearing of the bits required to complete the writing process<br><br>**Affected component:** INTEL TXE FW |
| 1304460062 | FW doesnt enter recovery at Swap step 6 | **Description:** CC partition didn't load from the BPDT2.<br><br>**Affected component:** INTEL TXE FW |
| 1404747976 | The following messages "USB Enumeration Timeout" and "DnX Ping Timeout" values not reflected in INTEL TXEInfo | **Description:** Even though the two are configurable in FIT, changing them won't be seen in INTEL TXEInfo.<br><br>**Affected component:** INTEL TXE FW |
| 1404837800 | Loading cse_image.bin is causing warning about invalid GPIO | **Description:** Using any of the cse_image.bin files (a0, b0, a0 rombypass, etc) produce this warning.<br><br>**Affected component:** INTEL TXE SW Tools |
| 1404890025 | BXT-P: INTEL TXEManuf produces warning for NFC when NFC is disable in config file | **Description:** Running the BIST using -f config file that has NFC disabled produces warning 298 for NFC.<br><br>**Affected component:** INTEL TXE SW Tools |
| 1404896721 | FIT crashes when building split SPI image with any flash size set to 64MB | **Description:** Building a split SPI image with flash sizes being 64MB and x (any value) is causing FIT to crash.<br><br>**Affected component:** INTEL TXE SW Tools |
| 1404906825 | When running INTEL TXEInfo post-EOM, the following error is thrown: 57 - Failed getting variable "NFC GPIO Select" value | **Description:** Need to update GPIO file permissionsso tools are able to read variables after EOM.<br><br>**Affected component:** INTEL TXE FW Tools |

| | | |
|---|---|---|
| 1404912638 | Updating and commiting Oem_tag and OemSkuRule along with INTEL TXEMeManufacturingModeDone using FPT, fails to update the values | **Description:** FPT does not update Oem_tag and OemSkuRule that are updated and commited along with INTEL TXEManufacturingModeDone.<br><br>**Affected component:** INTEL TXE FW |
| 1304419979 | PTT enters Failure Mode when signing with an external RSA key with bad private/public | **Description:** PTT enters failure mode instead of remaining operational.<br><br>**Affected component:** INTEL TXE FW |
| 1404960923 | INTEL TXEInfo is indicating wrong Secure Boot profile and does not match what was set in FIT | **Description:** INTEL TXEInfo indicates wrong Boot profile value and doesn't match other tools' value.<br><br>**Affected component:** INTEL TXE FW Tools |
| 1405012009 | FPT WRITETOKEN command is not unlocking the platform | **Description:** Platform should be unlocked when running WRITETOKEN –VERBOSE command<br><br>**Affected component:** INTEL TXE SW Tools |
| 1405016182 | Flash Programming Tool GETPID command creates an empty "PID" binary | **Description:** Flash Programming Tool "GETPID" command returns a Part ID with all 0's and creates an empty binary file.<br><br>**Affected component:** INTEL TXE SW Tools |
| 1405031166 | INTEL TXEManuf did not output pass with warning when using WarningContinue as ErrAction | **Description:** The final report by INTEL TXEManuf should be "Pass With Warning" instead of "Operation Failed".<br><br>**Affected component:** INTEL TXE SW Tools |
| 1304460514 | After sending the last chunk data of Verify Manifest MKHI command get response with Manifest sig invalid(0x0C00810C) | **Description:** Send "Verify Manifest" for IBB of the same burned image resulted in invalid Mainfest Sig.<br><br>**Affected component:** INTEL TXE FW |
| 1304472655 | Image check command results with FW connection is lost | **Description:** UPDATE_IMAGE_CHECK resulted in Zero Header instead of "Success 0x00".<br><br>**Affected component:** INTEL TXE FW |
| 1304435713 | PTT Leaves Failure Mode After S3 | **Description:** PTT should persist Failure Mode through S3 cycles<br><br>**Affected component:** INTEL TXE FW |



| | | |
|---|---|---|
| 1405022799 | FPT throws communication error with SPI operations in FDO mode in Windows | **Description:** A communication error occurred between FPT and INTEL TXE n FDO mode.<br><br>**Affected component:** INTEL TXE FW |
| 1405009438 | Platform will not boot if FPF DnX OEM ID is set to non-zero value (FPFs have not been committed) | **Description:** Platform didn't boot if OEM-ID was set to any non-zero value.<br><br>**Affected component:** INTEL TXE FW |
| 1304452202 | PTT: TPM is cleared when performing RTC clear | **Description:** TPM was cleared when performing RTC clear using jumper J384.<br><br>**Affected component:** INTEL TXE FW |
| 1404794657 | FIT, Region Order: unsupported EC region referenced in the Region order build setting | **Description:** EC region is not supported in APL and was removed from FIT.<br><br>**Affected component:** INTEL TXE SW Tools |
| 1404837043 | INTEL TXEManuf cfggen -all resulted in tests not relevant to APL showing up | **Description:** Wrong tests – not relevant to APL's architecture - could have been triggered confusing OEMs.<br><br>**Affected component:** INTEL TXE SW Tools |
| 1208244934 | INTEL TXEInfo need to update FWSTS-6 parser for FPF commit status | **Description:** INTEL TXEInfo parser code was updated from 1-bit allocation to 2-bits allocation<br><br>**Affected component:** INTEL TXE SW Tools |
| 1304473203 | TPM driver not functional until next boot during key generation stress testing | **Description:** cmdReady handshake duration sporadically exceeds 200ms cause TPM driver not functional until next boot<br><br>**Affected component:** INTEL TXE FW |
| 1304502361 | After modifying Anti-Reply (AR) file and table, loss of power causes failure in reading AR file | **Description:** The AR file would become unreadable in case power was lost.<br><br>**Affected component:** INTEL TXE FW |
| 1405064842 | FPT -dataclear on Post-EOM+Windows+SPI with FDO asserted does not clear FPT marker in Device Expansion region | **Description:** Flashing full image (-f) under same exact configuration does correct clear the device expansion region.<br><br>**Affected component:** INTEL TXE SW Tool |

| | | |
|---|---|---|
| 1405065012 | FPT flashing Bios/IFWI region on Post-EOM+Windows+SPI with FDO asserted does not clear FPT marker in Device Expansion region | **Description:** In post-EOM with FDO asserted, Device Expansion region's FPT marker is not being cleared.<br><br>**Affected component:** INTEL TXE SW Tool |
| 1404953617 | After closemnf, the following warning is thrown: "There are some addresses that are not defined in any regions" | **Description:** Running FPT –closemanuf results in Read/Write/Erase operations not applicable.<br><br>**Affected component:** INTEL TXE SW Tool |
| 1405099610 | Windows FPT command ERASETOKEN re-locks the platform, but returns a failure | **Description:** FPT re-locks the platform after running command "FPT... -VERBOSE -EraseToken", but throws an operation failure.<br><br>**Affected component:** INTEL TXE SW Tools |
| 1405142006 | FPT: Error Message "PMxdll.dll DebugMsg: Failed to SetThreadAffinity to 0x8 err:87" appears when FDO is asserted | **Description:** PMxdll.dll error message seen while running 'FPT -I' or 'FPT -F' when FDO is asserted<br><br>**Affected component:** INTEL TXE SW 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 |
|---|---|---|
| 1405010396 | USB Enumeration Timeout and Dnx Ping Timeout" does not accept values greater than 99. | **Description:** CVARs fail to accept values larger than 99.<br><br>**Affected component:** INTEL TXE SW Tool |
| 1405067496 | FPT -cfggen needs to remove unsupport features for OEMSkuRule & FeatureShipState CVARs from config file | **Description:** FPT -cfggen generated config file should remove AMT and NFC related info.<br><br>**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.<br><br>**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.<br><br>**Affected component**:INTEL TXE SW Tool |
| 1208423519 | FPT displays incorrect value for BootGurad in CFGGEN file | **Description:** Fpt -r BootGuard" prints the correct value "Profile 0 - Legacy" as the output, where as cfggen output prints it as "Pr" only<br><br>**Affected component:** INTEL TXE SW Tools |



# 4 Implemented RCRs

The following table lists implemented RCRs in this release.

| Issue # | Title | Description/ Affected component |
|---|---|---|
| 1206962007 | Migrate GPIO data from SMIP to NVAR and remove profile support. | **Description:** Using GPIO configuration data that is maintained as an NVAR with only one default profile.<br><br>**Affected component:** INTEL TXE FW & FW Tools |
| 1304355750 | Support for DATA CLEAR LOCK INTEL TXEI command (replaces HMRFPO LOCK) and DATA CLEAR DISABLE in FITC | **Description:** APL supports the equivalent to “HMRFPO LOCK” knobs that were available on previous platforms.<br><br>**Affected component:** INTEL TXE FW & FW Tools |
| 1304354545 | APL INTEL TXEManuf FPF EOL Tests | **Description:** Customers can enforce manuf requirements and ensure a feature is manufactured as desired.<br><br>**Affected component:** Manufacturing Tools & Services |
| 1208197638 | FIT tool updates to support PMC Feature Enable (remove 2nd cold reset) - new PMC OEM SMIP field | **Description:** FIT integrates new PMC OEM SMIP collaterals, OEM will be able to turn on/off the faster boot time.<br><br>**Affected component:** INTEL TXE FW Tools |
| 1207656970 | APL FPF Full Redundancy | **Description:** FFP layout for BXT was moved to full 3-bit redundancy to match TD redbook guidance<br><br>**Affected component:** INTEL TXE FW |
| 1504173680 | Maximize OBB size in IFWI design for larger BIOS size room to support customer needs | **Description:** Customer BIOS maximum sizes can be increased/decreased<br><br>**Affected component:** INTEL TXE FW |
| 1208188710 | FIT to enforce SPI descriptor FLCOMP fields (non-freq) and PMC OEM SMIP FLCOMP (nonfreq) fields match - to prevent OEMmisconfiguration | **Description:** OEM will no longer have to manually ensure that the non-freq fields of SPI descriptor FLCOMP and the same fields in PMC OEM smip FLCOMP match.<br><br>**Affected component:** INTEL TXE FW Tools |