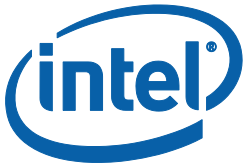

Gemini Lake Platform - Intel® Trusted Execution Engine (Intel® TXE) 4.0 Firmware

Release Notes - NDA

Revision 4.0.25.1324 – Maintenance Release

March 2020

Intel Confidential

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.

Revision History

Revision Number	Description	Revision Date
4.0.25.1324	Maintenance Release	March 2020
4.0.20.1311	IPU 2019.2 PV Release	August 2019
4.0.20.1310	Hot Fix Release	June 2019
4.0.20.1308	Maintenance Release	May 2019
4.0.15.1303 Version 3	Hot Fix Release	May 2019
4.0.15.1303 Version 2	Hot Fix Release	April 2019
4.0.15.1303	QSR 2019.1 PV Release	April 2019
4.0.10.1288v2	HF Release	February 2019
4.0.15.1290	QSR 2019.1 Beta Release	January 2019
4.0.10.1288	QSR 2018.4 RS5 PV Release	November 2018
4.0.10.1281	Beta RS5 Release	October 2018
4.0.5.1280	QSR PV Release	July 2018
4.0.0.1249 Version 3	PV Release - RS4	June 2018
4.0.0.1249	Hot Fix Release – RS4	May 2018
4.0.0.1245 Version 4	Hot Fix Release – RS3	March 2018
4.0.0.1245 Version 3	Hot Fix Release – RS3	February 2018
4.0.0.1245 Version 2	Hot Fix Release – RS3	February 2018
4.0.0.1245	Hot Fix Release – RS3	January 2018
4.0.0.1242	PV Release – RS3	January 2018
4.0.0.1235	PC Release – RS3	November 2017
4.0.0.1232	PV Release – RS2	November 2017
4.0.0.1218	BKC Release – RS2	September 2017
4.0.0.1192	BKC Release – RS2	August 2017
4.0.0.1189	BKC Release – RS2	July 2017
4.0.0.1187	BKC Release – RS2	June 2017
4.0.0.1184	Beta Candidate Release – RS2	May 2017
4.0.0.1181	Engineering Release – RS2	May 2017
4.0.0.1180	Engineering Release – RS2	April 2017
4.0.0.1170	Alpha Milestone Release – RS2	March 2017
4.0.0.1148	Engineering Release - RS2	January 2017
4.0.0.1143	Pre-alpha Release - RS1	January 2017

Contents

1 Introduction 6
1.1 Glossary 6
1.2 System Power States 7
1.3 Important Notes 7
2 Release Kit Details 10
2.1 Supported Operating Systems 10
2.2 VCN Firmware Upgrade / Downgrade Table 10
2.3 Kit content 11
2.3.1 Documents 11
2.3.2 Firmware and Installers 11
2.3.3 Tools 12
2.4 iCLS SW Change Log 13
3 Fixed issues in This Release 14
3.1 Mitigated Security Vulnerabilities 14
3.2 Validation Guidance 14
4 Implemented RCRs in This Release 16
5 Intel® TXE FW Known Issues 17
6 Intel® TXE SW Tools Known Issues 18
7 Archive 19
7.1 Fixed issues 19
7.2 Implemented RCRs 26

1 Introduction

This document covers Intel® Trusted Execution Engine firmware for the following platforms:

- Intel Pentium Silver processors N5000 for mobile and J5005 for desktop.
- Intel Celeron processors N4100 and N4000 for mobile and J4105 and J4005 for desktop.

1.1 Glossary

Acronym/ Terminology	Definition
BIOS	Basic Input Output System
BUP	Bring Up
EC	Embedded Controller
EDK	EFI Development Kits
EOM	End of Manufacturing
EOP	End of Post
FW	Firmware
HLK	Hardware Lab Kit
IBB	Initial Boot Block
Intel® DAL	Intel® Dynamic Application Loader
Intel® DnX	Intel® Download and Execute
Intel® FIT	Intel® Flash Image Tool
Intel® FPT	Intel® Flash Programming Tool
Intel® IPP	Intel® Integrated Performance Primitives
Intel® MEU	Intel® Manifest Extension Utility
Intel® OED	Intel® Offload Engine Driver
Intel® PFT	Intel® Platform Flash Tool
Intel® SPD	Intel® Storage Proxy Driver
Intel® SST	Intel® Smart Sound Technology
Intel® TXE	Intel® Trusted Execution Engine
Intel® TXEI	Intel® Trusted Execution Engine Interface
Intel® TXEInfo	Intel® Trusted Execution Engine Info tool
Intel® TXEManuf	Intel® Trusted Execution Engine Manufacturing tool
MCA	Manufacturing Configuration App
MSU	Mobile Signing Utility
OS	Operating System

Acronym/ Terminology	Definition
PAVP	Protected Audio Video Path
PMC	Power Management Controller
RCR	Requirements Change Request
SMIP	Signed Master Image Profile
SPI	Serial Peripheral Interface
SW	Software
USB	Universal Serial Bus

1.2 System Power States

State	Description
S0	**Power on** - A system state where power is applied to all Hardware devices and system is running normally.
S3	**Sleep/ Suspend** - A system state where platform keeps memory and other devices powered. OS state is saved to memory and resumed from memory when mouse, keyboard or other activity occurs that is configured as a wake event.
S4	**Hibernate** - A system state where most of power sources are off, the system saves the contents of memory to a hibernation file, preserving the state of the operating system, applications, and open documents.
S5	**Power Off** - A system state where all power to the host system is off and the power cord is still connected.
S0ix	**Active idle** - A system state which delivers the same power consumption as S3 sleep, but with a quick enough wake up time to get back into full S0.
G3	**Mechanical Off** - All Power source are disconnected.

1.3 Important Notes

- Intel® TXE 4.0.25.1324 has been updated to include functional and security updates. Users should update to the latest version.
- This Firmware Kit includes an updated version of the Intel® Content License Service (iCLS) Client Software version 1.59.241.0 which must be deployed with the firmware update.
- Please note that this Intel® CSE 4.0.25.1324 includes an implemented RCR . Please refer here for more details
- Please note that this release includes mitigation of Intel® TXE CVEs included in the forthcoming 2019.2 Intel Platform Update Security Release. Accompanying details will be provided under NDA after WW26 as part of the normal IPU disclosure process.

- Starting from Intel® TXE version 4.0.10.1288, Windows* 10 RS5 is supported.
- Customers are requested to always adopt Intel® TXE FW, Intel® TXE Drivers and Intel® TXE tools versions from the same kit. A mix between kits is not supported and might cause unexpected issues.
- Intel® IFWI required Firmware components include: Intel® TXE, OEM SMIP, CPU uCode patch, PMC FW patch. Please reserve space for the below noted components on SPI per each component maximum size.
- Intel® FW fixed SPI size:

Component	Size (KB)
BPDT/SBPDT x 2 +IFP + UEP	8
Descriptor	4
OEM SMIP	16
PMC patch	80
CPU uCode (single patch)	192
Debug Tokens	32
TXE RBE	64
TXE BUP	400
TXE Main	1280
TXE Data (Device Expansion Region)	512
Total	2588

Based on 8MB SPI storage limit, customer BIOS maximum sizes can be increased/decreased according to the configuration choice below:

Fixed Size	ISH	EC FW	BIOS Data	MAX Size Bios
2588	0	0	0	5604
2588	0	0	128	5476
2588	0	0	256	5348
2588	0	0	384	5220
2588	0	0	512	5092
2588	260	0	0	5344
2588	260	0	128	5216
2588	260	0	256	5088
2588	260	0	384	4960
2588	260	0	512	4832
2588	0	512	0	5092

Fixed Size	ISH	EC FW	BIOS Data	MAX Size Bios
2588	0	512	128	4964
2588	0	512	256	4836
2588	0	512	384	4708
2588	0	512	512	4580
2588	260	512	0	4832
2588	260	512	128	4704
2588	260	512	256	4576
2588	260	512	384	4448
2588	260	512	512	4320

Notes:

1. "MAX Size BIOS" = IBB + OBB.
2. BIOS Data =BIOS data reserved in TXE data region (DE region) configurable in FIT. If they choose "0", they may store their BIOS data in their BIOS regions.

2 Release Kit Details

The kit can be downloaded from VIP (https://platformsw.intel.com/). See the supported OS(s) and details on kit content below.

2.1 Supported Operating Systems

- Windows* 10 64 bit.
  Please talk to the Intel representative about other OS support.

2.2 VCN Firmware Upgrade / Downgrade Table

Intel® CSME FW Version	SVN Number	VCN Number	PV (1 or 0)
4.0.25.1324	1	8	1
4.0.20.1311	1	6	1
4.0.20.1310	1	6	1
4.0.20.1308	1	6	1
4.0.15.1303 *Version 3*	1	5	1
4.0.15.1303 *Version 2*	1	5	1
4.0.15.1303	1	5	1
4.0.0.1249 *Version 2*	1	4	1
4.0.10.1288	1	4	1
4.0.10.1281	1	4	1
4.0.5.1280	1	3	1
4.0.0.1249 *Version 3*	1	2	1
4.0.0.1249 *Version 2*	1	2	1
4.0.0.1249	1	2	1
4.0.0.1245 *Version 4*	1	2	1
4.0.0.1245 *Version 3*	1	2	1
4.0.0.1245 *Version 2*	1	2	1
4.0.0.1245	1	2	1
4.0.0.1242	1	2	1
4.0.0.1235	1	1	1
4.0.0.1232	1	1	1
4.0.0.1218	1	1	0
4.0.0.1192	1	1	0
4.0.0.1189	1	1	0
4.0.0.1187	1	1	0
4.0.0.1184	1	1	0
4.0.0.1181	1	1	0

Intel® CSME FW Version	SVN Number	VCN Number	PV (1 or 0)
4.0.0.1180	1	1	0
4.0.0.1170	1	1	0
4.0.0.1148	1	1	0
4.0.0.1143	1	1	0

- The VCN (Version Control Number) has been increased to 8, which prohibits downgrading to Intel® TXE FW with a lesser VCN.
- The SVN (Security Version Number) has been increased to 1, which prohibits downgrading to Intel® TXE FW with a lesser SVN.

2.3 Kit content

2.3.1 Documents

- Intel® TXE FW Bring Up guide – Revision 1.0
- Intel® TXE FW Bring Up guide "***Quick Start***" – Revision 1.0
- System Tools User Guide – Revision 1.2
- VSCCommn_binContent - Revision 5.0.2
- Signing and manifesting guide – Revision 1.1
- Secure Tokens Guide - Revision 1.1
- SMIP and SPI programming guide – Revision 1.22
- Intel® TXE FW 4.0.25.1324 Release Notes

2.3.2 Firmware and Installers

Type	Version
Intel® TXE Firmware	4.0.25.1324
MSI/ DCH Software Installer	2004.4.0.176
MUP Specification Version	2.4.4
Intel® Trusted Execution Engine Interface (Intel® TXEI) driver 64b	1924.4.0.1062 **Submission ID:** 1152921504628082885 **Shared Product ID:** 1152921504607715915

Type	Version
Intel® Storage Proxy Driver (Intel® SPD) 64b	1731.4.0.1199 **Submission ID:** 1152921504628051411 **Shared Product ID:** 1152921504607703039
Intel® Content License Service (Intel® iCLS)	1.59.241.0 **Submission ID:** 1152921504628273045 **Shared Product ID:** 1152921504607863002
Intel® OEM Extension	1924.4.0.1062 **submission ID:** 1152921504628082884 **shared product ID**: 1152921504607715914
Intel® JHI Driver	1.34.2019.0714 Submission ID: 1152921504628116402 Shared Product ID: 1152921504607732841

2.3.3 Tools

Tool	Version	Description
Intel® FIT	4.0.25.1325	• Flash Image Creation Tool • Provided as both, a GUI and a command line tool • OS Support: Windows* 7 (32-bit) and above
Intel® FPT	4.0.25.1325	• Command line tool • Writes the flash image into the SPI flash device • OS Support: Windows* 7 (32-bit) and above/ EFI
Intel® TXEInfo	4.0.25.1325	• Command line tool • Provides FW version information • OS Support: Windows* 7 (32-bit) and above/ EFI
Intel® TXEManuf	4.0.25.1325	• Command line tool • Validates Intel® TXE functionality on the manufacturing line • OS Support: Windows* 7 (32-bit) and above/ EFI
Intel® MEU	4.0.25.1325	• Command line tool • Generates binaries that contain manifests
Intel® PFT	5.9.5.0	• Provided as both, a GUI and a command line tool • Flashes FW, OS image and Modem FW on Intel® Platforms

Tool	Version	Description
		• OS Support: Windows* 7 (32-bit) and above/ Ubuntu
Mobile Signing Utility (MSU)	1.1.2	• Command line tool • Allows PFT to sign secure tokens • OS Support: Windows* 7 (32-bit) and above/ Ubuntu

2.4 iCLS SW Change Log

Intel® Capability License Service (iCLS) Client is included as part of the Intel® TXEI Driver Software installer package within the TXE FW Kits.

Note: Intel® Capability License Service (iCLS) requires internet connectivity over TCP/IP port 443; if the port is blocked by the network, iCLS cannot communicate with the iCLS Service Servers.

iCLS SW Version	Intel® TXE SW Version	Introduced in Intel® TXE FW Kit Version	Changes
1.59.241.0	2004.4.0.176	4.0.25.1324	• TSS updated to 2.3.1 • OpenSSL updated to 1.1.1d • gSoap updated to 2.8.95
1.56.87.0	1929.4.0.1070	4.0.20.1311	• OpenSSL updated to 1.1.1c • gSoap updated to 2.8.84 • TSS updated to 2.2.3
1.55.66.0	1919.4.0.1057	4.0.15.1303 Version 3	• gSoap updated to 2.8.83 • SDK/WDK/ADK updated to 19H1 10.0.18362.0 (RTM) • UWD INF installer certified for RS3,RS4,RS5 and 19H1. • Intel® PTT timeout of iCLSClient extended in Linux* version

3 Fixed issues in This Release

Issue #	Title	Details
1307025629	Flash log is filled out with irrelevant error logs in coinless designs	**Description:** In coinless designs, an RTC reset happens on each G3 resume flow causing Flog to be filled out with error messages of RTC reset **Affected Component:** Intel® TXE FW
1307236184	Intel PTT enters failure mode when saving HMAC sequence	**Description:** Due to intel PTT data size being larger than the buffer size, and this leads to the PTT entering in failure mode when using HMAC sequence. **Affected Component:** Intel® TXE FW
1607379724	System shows an error when using Intel® FPT tool from Intel® TXE 4.0.20.1308 kit	**Description:** **The** system shows an error "Setting Global Reset fail" **Affected Component:** Intel® TXE tools

3.1 Mitigated Security Vulnerabilities

This section describes security issue mitigations in Intel® TXE in this Intel Release.

Release	Technical Advisory (TA)	Doc #	Reference Details
Maintenance	PSIRT-TA-PSIRT-TA-2019-10-001	615340	2020.1 MR – Intel® CSME, SPS, TXE, AMT and DAL, PSIRT-TA-2019-10-001
2019.1	PSIRT-TA-201901-002	607858	Intel® Converged Security Management Engine (CSME) QSR 2019.1
2018.4	PSIRT-TA-201810-004	603440	Intel® Converged Security Management Engine (CSME) QSR 2018.4.
2018.2	PSIRT-TA-201805-001	597108	Intel® Converged Security Management Engine (CSME) QSR 2018.2.

3.2 Validation Guidance

This document provides detailed validation guidance associated with this Intel Release.

Release	Doc #	Reference Details
Maintenance	618465	Intel® CSME Firmware and Intel® TXE Firmware Intel Platform Update Security Update Beta
2019.1	608852	Intel® CSME Firmware and Intel® TXE Firmware QSR 2019.1 Validation Guidance
2018.4	604339	Intel® CSME Firmware and Intel® TXE Firmware QSR 2018.4 Validation Guidance

§§

4 Implemented RCRs in This Release

RCR Number	Title	Description
1306993589	Restrict access to USB3 DbC after EOM	**Background** • This RCR aims to enhance the SoC security by adding some restrictions for debug using USB3 DbC. • Currently Intel® CSE supports debug capabilities for the platform before and after the EOM flow with no limitations. **Change Details** • DCI devices, including BSSB (CCA) and Dbc, will not be able to connect when the platform is locked after EOM. • In order to enable USB3 DbC, customers will need to first unlock the platform using an Intel or OEM token Please refer to ARB doc communication (617164) for more details
1306993589	ARB Physical Anti-rollback	**Background** The purpose of this RCR is to have a HW based ARB solution for Intel® CSE core modules and loadable modules which can later be extended,To prevent Intel® CSE runtime FW with old ARB SVN from running on a platform where newer ARB SVN has been written to FPF. **Change Details** ▪ Intel® CSE provides direct HW Based ARB protection through dedicated FPF and is controlled by Intel® OEM via FPF enabling/disabling setting. Default is permanently disabled ▪ MEInfo shall display this configuration ▪ Intel® CSE is configured with FPF based SVN verification : ▪ for OEM KM . Intel® CSE shall verify OEM KM manifest SVN value against the FPF stored SVN value.Intel® CSE shall continue to boot only in case the SVN in manifest is greater or equal to the value in FPF. ▪ when loading ucode patch, Intel® CSE shall verify ucode patch SVN value against the FPF stored SVN value. ▪ Tools changes: ▪ Intel® FIT shall have a single enable/disable for HW based ARB as a whole. Intel® MEInfo shall display the value in the FPFs.

§§

5 Intel® TXE FW Known Issues

Issue #	Title	Description/ Affected component
1504736825	Event viewer shows an error during S4 stress test or Warm Boot	**Will Not Fix** **Description:** OED Audio driver yellow bang is detected while executing S4 Stress test / Warm boot. **Workaround:** Disable and re-enable OED Audio driver or Rebooting system. **Affected Component:** Intel® TXE FW
1305203387	BSOD while running power management tests	**Description: [eMMC Only]** BSOD SDBUS_internal_error was captured while running cold reset, warm reset and S5 stress tests **Affected Component:** Intel® TXE FW
1305506365	Some log messages may be lost when Intel® TXE does not have access to write to the flash	**Will Not Fix** **Description: [eMMC Only]** When booting via eMMC or UFS, Intel® TXE does not have access to write to the flash all the time. This causes some messages to be lost. **Affected Component:** Intel® TXE FW
1305041558	The platform performs a global reset instead of S3/S4/S5 in an open DAL session.	**Will Not Fix** **Description: [SPI only]** Performing S3/S4/S5 in an open session of a DAL applet causes the platform to perform a global reset instead. **Affected Component:** Intel® TXE FW

§§

6 Intel® TXE SW Tools Known Issues

Issue #	Title	Description/ Affected component
1805519881	The EOM file is written regardless of the failure to run –closemnf	**Will not fix** **Workaround:** This issue is seen in negative flows only. Please make sure to update the BIOS settings properly. **Description: [SPI only]** EOM flow is being executed on the next boot after a failed –closemnf operation. This results in an undefined system state. **Affected Component:** Intel® TXE SW Tools
1304712165	No drop down box is available for Rail SVID ID parameters in the CPU Straps feature tab in Intel® FIT	**Will not fix** **Workaround:** Please input valid values only as text. **Affected Component:** Intel® TXE SW Tools
1304712246	No error message is shown when using Intel® FIT to build an image without a PMC sub-partition	**Will not fix** **Description:** When building an image without setting the PMC binary (an illegal build), no error message will be generated to the user. **Affected Component:** Intel® TXE SW Tools
1304712352	Flashing an Intel® FIT decomposed BIOS image fails to boot back the system upon global reset	**Will not fix** **Workaround:** Flashing a full image will prevent this issue from reproducing. **Affected Component:** Intel® TXE SW Tools
1304786443	Failure to run EFI system tools	**Will not fix** **Description:** Known issue across all platforms that were built with EDK **Workaround:** Need to put the vsccommn.bin or fparts.txt files in root directory, e.g. C: **Affected Component:** Intel® TXE SW Tools
1304926756	LSPCON support is still an option in Intel® FIT.	**Will not fix** **Description:** The option for using LSPCON in Intel® FIT is still available although it is not used as Intel® GLK Platforms support HDCP in hardware natively. **Affected Component:** Intel® TXE SW Tools

7 Archive

7.1 Fixed issues

Issue Number	Title	Details	Fixed in Kit Number
1507142160	CVT Tool Check fails with software from Intel ® TXE 4.0.15.1295	**Description:** CVT Tool shows a red error message for failure in driver MUP Check. **Affected Component:** Intel® TXE SW	4.0.12.1311
1409308277/ 1507181322	Uninstalling Intel® TXE driver is not working properly.	**Description:** Uninstalling Intel® TXE driver ends successfully, however an error message is being displayed. **Affected Component:** Intel® TXE SW	4.0.12.1311
1507181322	Uninstalling Intel® TXE driver is not working properly.	**Description:** Uninstalling Intel® TXE driver ends successfully, however an error message is being displayed. **Affected Component:** Intel® TXE SW	4.0.15.1303 Version 3
1306115380	Intel® PTT enters failure mode whilst transitioning from PK-TPM.	**Description:** Intel® PTT enters failure mode whilst transitioning from PK-TPM if there's no locality granted or if a startup has been sent. **Affected Component:** Intel TXE FW	4.0.15.1303
1504762498	"Return codes" duplication occurs in metadata info.	**Description:** N/A **Affected Component:** Intel TXE Installer	4.0.15.1303
1507142160	CVT returns "DAL_WC.inf specified in the content node not found in extracted content" error in the DCH installer	**Description:** N/A **Affected Component:** Intel TXE Installer	4.0.15.1303
1306089982	Calling TPM2_GetCapability fails when platform policy and lockout policy are not set.	**Description:** N/A **Affected Component:** Intel TXE FW	4.0.15.1303
1305965058	Intel® FIT doesn't expose the "ec_max_io_mode" configuration.	**Description:** N/A **Affected Component:** Intel TXE Tools	4.0.15.1303
1306089982	Calling TPM2_GetCapability() for capability TPM_CAP_AUTH_POLICIES with platform and lockout	**Description:** executing "PttTest.exe –t Test_Intel_GetCapability2 –tc AuthPolicies" command should return 4 policies; *Owner*, *endorsement*, *platform*, and *lockout*, with	4.0.15.1290

Issue Number	Title	Details	Fixed in Kit Number
	policies not set fails to return the full policies list.	platform and lockout policies empty. Instead, the platform and lockout policies are missing. **Affected Component:** Intel® TXE FW.	
1305965058	Intel® FIT Tool should expose the maximum IO Mode configuration.	**Description:** Intel® FIT Tool should expose the maximum IO Mode (Single/Dual/Quad) configuration of the eSPI bus that is supported by the eSPI master and specific platform configuration. **Affected Component:** Intel® TXE SW Tools.	4.0.10.1288
1306000388	Wrong device ID is being displayed in Fparts.txt	**Description:** the device ID in the Fparts.txt file is wrong, it has an extra '0' digit (0x2007017), whilst it should be (0x207017). **Affected Components:** Intel® TXE SW Tools.	4.0.10.1288
1305804186	Intel® PTT Sequence Commands return TPM_RC_VALUE	**Description:** Intel® PTT Sequence Commands return TPM_RC_VALUE instead of TPM_RV_MODE for a persistent handle. **Affected Component:** Intel® TXE FW.	4.0.10.1281
1806301786	After global reset PRTC nonce gets reset.	**Description:** While unlock mode and after performing global reset, token will be rejected as a result of nonce mismatch. **Affected Component:** Intel® TXE FW.	4.0.10.1281
2007591178	Closemnf command cannot be executed successfully because "BIOS Lock" is enabled by default.	**Description:** using a sharing SPI for EC FW means that different host/bios values are being used, which causes the SPI region to be locked as expected but the OEM bit is not set. **Affected Component:** Intel® TXE SW.	4.0.10.1281
1305332204	Intel® MEU doesn't generate OEMUnlockToken Config file.	**Description:** When executing –gen OEMUnlockToken in Intel® MEU, an OEMUnlockToken config file is not generated. **Affected Component:** Intel® TXE SW Tools	5.0.0.1249
1305657097	Crypto not receiving control over the HW.	**Description:** Crypto is waiting for ever for receiving control on the HW but does not get it. **Affected Component:** Intel® TXE FW Tools	5.0.0.1249
1305643715	Help text is wrong for enable split OBB. If users enable OBB splitting, the primary location is BP1, remaining extra OBB portion will be placed in BP2.	**Description:** it's actually the other way around, OBB's primary Location is in BP2 "Boot Partition 2" not BP1, if users enable Splitting OBB sub-partition, remaining extra OBB portion will be placed in BP1 **Affected Component:** Intel® TXE FW Tools	5.0.0.1249
1305595307/ 2201959455	Close Manufacturing process fails.	Description: Intel® FPT fails to set the manufacturing mode done bit. Affected Component: Intel® TXE SW Tools	4.0.0.1245 Version 2

Issue Number	Title	Details	Fixed in Kit Number
2202120409	Intel® FPT closemnf fails showing BIOS lock error.	Description: When using Intel® FPT version 4.0.0.1244 released in the previous Intel® TXE 4.0.0.1245 HF, close manufacturing process fails on BIOS lock detection. Affected Component: Intel® TXE SW Tools	4.0.0.1245 Version 2
1305550332	Intel® FPT updates the OEM ID with a wrong value in case the input value format was "0x000X"	Description: Intel® FPT sets a different value for the OEM ID instead of the user defined one in case the input value format was "0x00X". Affected Component: Intel® TXE SW Tools	4.0.0.1245
1305514331	Intel® TXE FW exception when trying to re-burn the IFP fuses	Description: Intel® TXE FW exception happens when running Intel® FPT closemnf process on a previously closed platform. Affected Component: Intel® TXE FW	4.0.0.1245
1504654058/ 2201429453/ 2202120081	Failure to run Intel® TXEManuf EOL check using Intel default SPI image configuration	Description: [SPI only] Failure to perform end of line check with Intel recommended configuration due to having the wrong default values for the EC read/write accesses in Intel® FIT. Affected Component: Intel® TXE SW Tools	4.0.0.1242
1305333688	Intel® FIT configurations for SATA m-PHY lane ports and GPIO signals do not match GLK platform design guide	Description: According to GLK platform design guide, there should be 2 SATA m-PHY lane port configurations and 2 GPIO signal configurations enabled in Intel® FIT. Affected Component: Intel® TXE SW Tools	4.0.0.1242
1305345538	Intel® FPT ME commands return success results after running Intel® FPT –DisableME	Description: [SPI only] ME commands in tools are not relevant to Intel® TXE based platforms. Affected Component: Intel® TXE SW Tools	4.0.0.1242
1305351613	Playready is accessing invalid memory when the received context is corrupted	Description: [SPI only] The FW fails to create a PAVP session when corrupted context is received. Affected Component: Intel® TXE FW	4.0.0.1242
1305413103	Intel® PTT persistent keys are lost after performing several system reboots	Description: [SPI only] Intel® PTT persistent keys are inaccessible after performing several continuous system reboots. Affected Component: Intel® TXE FW	4.0.0.1242

Issue Number	Title	Details	Fixed in Kit Number
1305226091	System goes into a loop of resets after running Intel® TXEManuf	Description: [eMMC Only] System goes into loop of resets after running Intel® TXEManuf twice on EFI shell over eMMC. Affected Component: Intel® TXE FW	4.0.0.1242
Important Update	Intel® TXEI driver	MSFT Signed Drivers	4.0.0.1235
1305182331	Failure to set EOP when performing Intel® TXE Compliance Test	Description: EOP is unable to set when using during compliancy testing Affected Component: Intel® TXE FW	4.0.0.1235
1305180842	Connected Standby stress test fails after ~430 iterations	Description: [eMMC Only] stress test fails due to DAL issue. Affected Component: Intel® TXE FW	4.0.0.1232
1305330446	Intel® TXEI and SPD drivers are signed by Intel Corporation and not by Microsoft*	Affected Component: Intel® TXE SW	4.0.0.1232
1305330652	Results for running Intel® TXEManuf EOL command are printed repeatedly a number of times	Description:[SPI only] Affected Component: Intel® TXE SW Tools	4.0.0.1232
1305133396	Failure to run Intel® TXEManuf tool while in EFI shell	Description: [eMMC only] Timeout of Intel® TXEManuf tool run command. Affected Component: Intel® TXE SW Tools	4.0.0.1232
1305046454	DRM issue	CVSSv3 is 6.2 (Medium) Affected Component: Intel® TXE FW	4.0.0.1218

Issue Number	Title	Details	Fixed in Kit Number
1305130640/ 1305060564	Asserting the FDO jumper causes the platform to hang	Description: [SPI only] Platform hangs on Post Code 0090 when having the FDO jumper asserted. Affected Component: IAFW.	4.0.0.1218
1305283768/ 1305283720	Intel® TXE system tools and DnX Dll file are not digitally signed by Intel	Affected Component: Intel® TXE SW Tools	4.0.0.1218
1305169490/ 1604282612/ 1604397870	Yellow bang observed on Intel® SST OED driver after waking from sleep (S3)	Description: Mis-synchronization between drivers causes driver timeout. Affected Component: Intel® TXE FW	4.0.0.1218
1305232328	Unable to erase invalid Anti-Replay files from flash after performing CMOS/G3 powerflow on a coinless platform	Description: [SPI only] Affected Component: Intel® TXE FW	4.0.0.1192
1305063698	Global reset was captured after ~200 iterations of S3 stress test	Description: [eMMC only] running s3 stress test Affected Component: Intel® TXE FW	4.0.0.1189
1305069910	Platform shuts down instead of resetting after flashing BIOS	Description: Running the command "FPT-greset" after flashing BIOS via Intel® FPT tool results in a shutdown instead. Affected Component: Intel® TXE SW Tools	4.0.0.1189
1305041509	System hangs on Intel® TXEI Driver test.	Description: [eMMC only] System hangs with blue screen while running device test Affected Component: SPD Driver	4.0.0.1189
1305124583	Unable to change "PTTEnable" CVAR.	Description: Unable to change "PTTEnable" CVAR in Intel® FPT configuration Affected Component: Intel® TXE SW Tools	4.0.0.1189

Issue Number	Title	Details	Fixed in Kit Number
1305096802	Intel® PTT versioning change.	Description: Intel® PTT versioning will be represented by major version (PTT generation) and minor version HW/Project identification) e.g: 400.1. starting with TXE FW 4.0.0.1189 PTT FW version will be 400.0.0.0 Affected Component: Intel® TXE SW Tools	4.0.0.1189
1305137941	Soc ConfigLock returns success even though it's not locked.	Affected Component: Intel® TXE SW Tools	4.0.0.1189
1304957146	Delayed resume of system state S3	Description: [eMMC Only] On S3 resume, the code is being prosessed instead of using the already existing code in DRAM. This causes a delay of ~250 msec. Affected Component: Intel® TXE FW	4.0.0.1187
1305056565	Intel® PTT becomes unresponsive when the SPD driver is not installed	Description: [eMMC Only] Intel® PTT stops responding when booting to Windows* OS via eMMC and the SPD driver is not installed. Affected Component: Intel® TXE FW	4.0.0.1187
1305031147	Failing of HDCP 2.2 during testing.	Description: Repeater topology verification fails after authentication. Affected component: Intel® TXE FW	4.0.0.1184
1305036404	Intel® FIT tool was programming wrong values for SPI Dual and Quad Read parameters.	Description: The SPI and SMIP Programming guide correctly states that SpiDualIOReadEnable should be disabled, while QuadIOReadEnable should be enabled as opposite to what was programmed via Intel® FIT tool. Affected Component: Intel® TXE SW Tools	4.0.0.1184
1305044861	Global reset performed while running S4 stress test.	Description: [SPI only] Global reset is captured in logs after running about 250 iterations of S4 stress test. Affected Component: Intel® TXE FW	4.0.0.1184
1304937282	Intel® TXEInfo tool displays incorrect FW version.	Description: Running TXEInfo is showing the FW version as 0.0.0.0 instead of returning the actual FW version value. Affected components: Intel® TXE SW Tools.	4.0.0.1181

Issue Number	Title	Details	Fixed in Kit Number
1305018896	Manufacturing mode closed only after running the command "fpt-closemnf" twice.	Description Intel® FPT tool reports that the manufacturing bit was set successfully but when the image is dumped the FW does not show any indication that fpt-closemnf was run. Manufacturing mode is closed only after global reset is executed and FPT –closemnf is run again. Affected Component: Intel® TXE SW Tools	4.0.0.1181
1304841858	Intel® FIT enables configuring EOM when setting only two out of four access permission values to the recommended values.	Description: Intel® FIT should enable EOM in its configuration when all four access permission values (read & write accesses for both the CPU and TXE) are set to the recommended values. Affected components: Intel® TXE SW Tools.	4.0.0.1180
1304752988	Wrong Intel® TXE driver version appears in Device Manager	Description: Intel® TXEInfo tool and Device Manager displays the wrong version of Intel® TXE driver. Affected components: Intel® TXE FW.	4.0.0.1170

7.2 Implemented RCRs

RCR #	Title	Description	Implemented in Kit #
2204835710	Intel® FIT Tool will support the ability to assert/de-assert the eMMC reset.	Intel® FIT Tool will support the ability to configure the eMMC reset per platform, where it could be asserted or de-asserted in Sx. This can be done in the platform configuration section in Intel® FIT Tool.	4.0.10.1288
1305989872	Supporting the ability to enable/disable flash Write Protection (WP) register values.	Intel® TXE ability to disable flash protection removal is now supported by adding a new configuration option to disable the "Write Protect" register values override. Note: Default value is set to the current Intel® TXE override behavior and this option can be configured by setting bit "28" at offset 0x11C.	4.0.10.1288
1605361265	Added Support for OEM customizable master access control in Intel® FIT, Intel® FPT, and Intel® TXEManuf tools.	Customers can now define their customized master access permission in Intel® FIT. Customers can also use Intel® FPT –closemnf command to apply these values. Intel® TXEManuf master access test will compare to the user defined values. **Note:** more information will be available soon in the next revision of the system tools user guide.	4.0.5.1280
220116037	Intel® MEU tool to support new XML configuration.	A new mechanism to enable skipping Data Modules from the hashing process has been introduced. <SkipHashModule> tag allows for more than one entry, only under the OBB sub-partition, to be excluded from hashing. Note: The previous flow used by Intel® MEU tool obliging the NVStorage Data Module to be placed at the end of the OBB sub-partition in order to exclude it from hashing is still a valid flow and can be used regardless of the new tag addition.	4.0.0.1245v2
1405281893	Support Linux* based Intel® FIT and MEU tools for systems with Ubuntu* OS	This release includes added Linux based Intel® FIT and MEU tools to enable creating and signing the flash image on Ubuntu* OS.	4.0.0.1242
1304688430	Dropped support for USB Cable Connection detection for Intel® TXE DnX trigger	Removing support for USB Cable Connection detection decreases boot time wait.	4.0.0.1184

RCR #	Title	Description	Implemented in Kit #
1604294451	MEEN is set on every boot pre EOM and when BSSB is connected to prevent Intel® TXE FW from enabling EXI during boot flow.	Intel® TXE FW used to enable EXI in boot flow even if it was disabled in BIOS. This affected the eXtensible Host Controller Interface (xHCI). Therefore, USB and type C ports became unfunctional when hot plugging USB devices in S4 system state.	4.0.0.1181
1304626755	Remove GPIO Configuration tab in Intel® FIT.	Moved "GPIO Straps" & "GPIO SSC Straps" configuration under "Platform Configuration" tab and removed the "GPIO Configuration" tab.	4.0.0.1180
1504367482	Remove ISH functionality from Intel® TXEInfo & TXEManuf.	Separated ISH functionality from Intel® TXEInfo and TXEManuf tools. ISH tools will be used now for ISH functionality.	4.0.0.1180
1304657897	Changed Intel® TXE SW kits versioning.	Intel® TXE SW installer's versions were changed to a new sequence format differs from Intel® TXE FW versioning to keep it clear distungish between the two installers.	4.0.0.1170

§§