Intel® Trusted Execution Engine (Intel® TXE) 1.0 FW

WW37’13 HF2v2
Intel® TXE FW Version 1.0.2.1060
General Notes

Legal Disclaimer

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document 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.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

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

Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. See www.intel.com/products/processor_number for details.

Intel® Platform/Device Protection Technology - No computer system can provide absolute security. Requires an enabled Intel® processor, enabled chipset, firmware, software and may require a subscription with a capable service provider (may not be available in all countries). Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. Consult your Service Provider for availability and functionality. For more information, visit http://www.intel.com/go/anti-theft . Consult your system manufacturer and/or software vendor for more information.

Code names featured are used internally within Intel to identify products that are in development and not yet publicly announced for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user.

Intel, Pentium, Celeron, and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

Table of Contents

- Intel® Trusted Execution Engine (Intel® TXE) HF2v2 Firmware version 1060 General Overview
- Fixed Intel TXE FW Issues
- Important Notes
- Manufacturing Flow
- Compliance Kit

Intel® Trusted Execution Engine 1.0.2.1060 - General Overview

- Intel® TXE 1.0.2.1060 Hot Fix2 version 2 firmware is posted to VIP.
- Kit #100462
- Customers must use Bay Trail BIOS Reference Code Rev 1.03 and CRB BIOS v51_31

Fixed Intel® TXE FW Issues

Issue #	Description	Impact/ Status
216728	fpt.efi asserts / fpt not working[1]	**Affected Component:** EFI FPT Tool. **Problem**: Upon running the following steps, FPT command will fail. Observe error message: assertion "tmp != NULL failed: file "sys\open.c", line 171 **Impact**: FPT will not be able to access SPI. **Root cause**: UEFI variable buffer size is too small. **Status**: Issue is fixed in FPT tool. Expected in next HF.

Note 1: Maximum EFI environment variable size supported by BIOS and Intel TXE manufacturing tools is 136KB (0x22000). Anything beyond this specification is neither supported nor validated. It is recommended to stay below this limit to avoid unexpected EFI and manufacturing tools behavior.

Fixed Intel® TXE FW Issues

Issue #	Description	Impact/ Status
4684330	All USB devices re-enumerate upon S3 resume when there is USB3.0 device connected to the USB3.0 external port	**Symptom:** • When there is a USB3.0 device connected to the USB3.0 external port, all USB devices connected to external USB ports will re-enumerate upon S3 resume. • This re-enumeration does not occur with USB2.0 devices connected to USB2.0 or USB3.0 ports or a USB3.0 device that is connected to a USB2.0 port. • This symptom will only happen before FPT –closemnf is set. **Impact:** Cannot run USB3 tests on resuming from S3 before closing manufacturing **Issue is Fixed in Intel TXE FW and available in this kit**
4999462	Intel® TXEI driver 1.0.0.1050 from Intel® Trusted Execution Engine Firmware 1.0.0.1058 HF1 kit is not WHQL.	**Symptom:** Intel® Trusted Execution Engine Interface (Intel® TXEI) driver 1.0.0.1050 from Intel® Trusted Execution Engine Firmware 1.0.0.1058 HF1 kit is not WHQL. **Impact:** WHKL test fails **Issue is Fixed in this kit**
216687	TXEManuf - MicroKernel - Internal Hardware Tests failed	**Symptom:** When using signed PV Intel TXE Firmware with Pre Production B2 Silicon parts, TXEManuf MicroKernel test will fail. **Impact:** TXEManuf.exe operation fails. **Workaround:** Pre-Production not signed Intel TXE Firmware is provided in HF2 kit to enable testing/ debugging with Pre Production Silicon parts. **Note:** This is an expected behavior. Customer expected to use Production B2 Silicon parts with signed PV Intel TXE Firmware.

Important Notes

1) Intel® Platform Trust Technology (Intel® PTT) is not POR for future Intel® Pentium® processor or Intel® Celeron® processor N- & J- Series based platform (formerly Bay Trail-M/D platform)

Since this configuration is not supported, customers are required to make sure Intel PTT is disabled in BIOS following the FRC and Intel TXE BWG instructions preventing end customer access to Intel PTT options through BIOS control.

2) Using EFI System Tools in UEFI Shell.

- Due to Microsoft's 'Mandatory UEFI Shells and related applications' requirement (System.Fundamentals.Firmware.UEFISecureBoot) when running Intel or customer manufacturing utilities in UEFI shell, the customer is required to disable UEFI Secure boot via BIOS setup menu or UEFI variable. If OEM/ODM wants to run specific EFI tool that needs to run with UEFI secure boot, OEM/ODM will sign that EFI tool with their OEM key

Important Notes

3) Intel TXE PV Firmware is signed by Intel

- PV POR configuration is signed Intel TXE FW and Production Silicon
- Signed Intel TXE FW and Pre Production Silicon is supported for development needs only and has the following limitation:
  - TXEManuf Micro Kernel test is not meant to run in this configuration. Therefore, this test is expected to fail.

Note: In HF2 kit, Unsigned Pre-Production Intel TXE FW is provided for Development and Testing needs with Pre Production Silicon.

Combination of unsigned Intel TXE Firmware and Production Silicon is not supported and will result in unexpected behavior

Important Notes

4) The VCN (Version Control Number) value has been increased in HF1 to '2'. As a result, Full FW upgrades from earlier releases are possible. However, a downgrade from 1.0.0.1058/ 1.0.2.1060 to PV Release or earlier is not possible.

5) Manufacturing Recommendation document has been updated with changes to Manufacturing Repair Process Flow (IBL # 526064)

Field Programmable Fuses - Manufacturing Flow

- Field Programmable Fuses are write-once, non-volatile memory. When FPFs are committed, the changes are permanent and irreversible.
- Bay Trail M/D customers are requested not to test, use or modify the FPF default values as there are no POR FW features that utilize FPF.
- FPF default values should be committed at EOM using FPT – WRITEGLOBAL command before closing manufacturing.
- FPT – closemnf command will fail if FPT – WRITEGLOBAL was not committed

Note: Mfg. flow for Bay Trail-M/D platform is different than Bay Trail-T platform.

Customer expected to follow Manufacturing Recommendations. IBL # (526064)

Bay Trail-M/D Intel® TXE Compliance Kit

- **What is the Intel Platform Compliance Kit?**
- A single kit with multiple tools for Bay Trail-M/D Compliance testing:
  - OEMs are requested to test/verify/confirm various Intel® TXE FW compliance tests with these tools
  - Tools for debugging (Intel® System Scope Tool)
- Each major milestone release will include:
  - Intel® Platform Enablement Test Suite, Intel® Automated Power Switch, Intel® System Scope Tool, and other tools to be included
  - User Guides, Compliance Test Results, Release notes and latest Compliance Guide
- The Bay Trail-M/D Intel TXE PV Compliance Kit release is available on VIP – Kit # 54724