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

Intel® TXE FW 1.0.2.1060 Production Version Release for Windows* 8.1 64-bit NCS

General Notes

WW43, October 2013

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.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

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

This document contains information on products in the design phase of development. Do not finalize a design with this information. Revised information will be published when the product is available. Verify with your local sales office that you have the latest datasheet before finalizing a design.

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.

All 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.

All products, computer systems, dates and figures specified are preliminary based on current expectations, and are subject to change without notice.

Intel 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.

Other names and brands may be claimed as the property of others.
All products, computer systems, dates and figures specified are preliminary based on current expectations, and are subject to change without notice.

Table of Contents

Intel® Trusted Execution Engine 1.0.2.1060 - General Overview

- Intel® TXE 1.0.2.1060 Production Version firmware for Windows* 8.1 64-bit NCS is posted to Intel® VIP
  - Intel® Trusted Execution Engine Production Version 1.0.2.1060 for Bay Trail-M/D
  - Kit # 100506
  - FITC Tool SSC% functionality added. Refer to Bring Up guide.

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 this 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) 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 Windows* 8.1 Bay Trail-M/D Intel TXE PV Compliance Kit release will be available on VIP – Kit # 56324