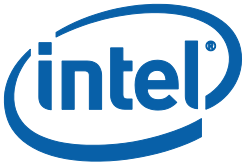

Bay Trail M/D Platform – Intel® Trusted Execution Engine (Intel® TXE) FW

Firmware Release Notes

Windows* 8 32-bit &64-bit HF2v2 Release

September 2013

Intel Confidential

Contents

§

1 Introduction

1.1 Scope of Document

This document provides component level details of the downloaded kit and the contents of each folder in the kit.

1.2 Acronyms

Term	Description
FITC	Flash Image Tool Creation
FPT	Flash Programming Tool
Intel® TXE	Intel® Trusted Execution Engine (Intel® TXE)
Intel® TXEI	Intel® Trusted Execution Environment Interface

§

2 Release Kit Summary

This document covers the following Intel® Trusted Execution Engine (Intel® TXE) Firmware release notes for future Intel® Pentium® processor or future Intel® Celeron® processor N- & J- series based platform (formerly Bay Trail-M/D platform).

2.1 Contents of Downloaded Kit

2.1.1 Documents

- Bay Trail–M/D platform Intel® TXE FW Bring Up Guide
- Intel® TXE System Tools User Guide
- Bay Trail–M/D platform - Intel® TXE FW Release Notes
- VSCCommn.bin Content

2.1.2 Tools

Tool	Description
FITC	• Flash Image Creation Tool • Provides both a GUI and a command line tool. • OS Support – Windows* 7 (32-bit) and Windows* 8
FPT	• Flash Programming Tool • Tools Provided within Windows command line tool.
TXEInfo	• Intel TXE setting checker tool
TXEManuf	• Validates Intel TXE functionality on manufacturing line
FWUpdate	• Updates the Intel TXE FW code region on a flash device that has already been programmed with a complete SPI image

2.1.3 Versions

Type	Version
Intel® TXE FW	1.0.2.1060
Intel® TXEI driver	1.0.0.1050
BIOS	BayTrail_DM_Release_v51_31x32.ROM BayTrail_DM_Release_v51_31x64.ROM

§

3 Important Notes

- It is highly recommended to use the FITC tool provided in this kit.
- Please make sure to use Intel TXE FW and system tools from the same kit. Versioning combinations might cause unexpected issues.
  - Please use SPI Flash parts that align with the Bay Trail Platform SoC SPI Flash Compatibility Requirements document (IBL# 514482, section 3)
- HF2v2 Engineering kit supports the following:
  - Booting with Intel TXE Enabled
  - Windows* 32 & 64 bit and EFI32 & 64 bit System Tools
  - Intel® Trusted Execution Engine Interface (Intel® TXEI) driver installer
- Please note that CRB BIOS image is not provided in Intel TXE FW kit. It can be downloaded as part of the CRB BIOS image release.
- Please note this kit is aligned with Bay Trail-M/D Platform Windows 8 64 Bit Non-Connected Standby PV Best Known Configuration
- BIOS release notes are part of the Bay Trail M/D platform, Bayley Bay - Customer Reference Board BIOS Image kit
- The VCN (Version Control Number) value has been increased in HF2 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.

§

4 Issues Fixed

4.1 Firmware

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 TXE Firmware with Pre Production B2 Silicon parts, TXEManuf MicroKernel test will fail. **Impact:** TXEManuf.exe operation fails. **Workaround:** Pre-Production not signed 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.
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.

§

5 Known Issues

5.1 Firmware

Issue #	Description	Affected Component/Impact / Workaround/Status
216744	FPTw: fail to perform -closemnf on prelock SPI image	**Affected Component:** EFI FPT Tool. **Problem:** Closemnf fails when using Pre Lock SPI image **Root cause:** FPT - WRITEGLOBAL need to be set before closemnf. **Workaround:** Please follow this manufacturing flow when using pre-lock SPI image: Build SPI image with pre-lock enabled (FITC)-> TXEManuf (TXE selftest) -> your test step -> FPT –writeglobal -> TXEManuf –EOL

§