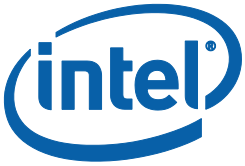

Bay Trail M/D Platform – Intel® Trusted Execution Engine (Intel® TXE) FW

Firmware Release Notes

Windows* 8.1 64-bit Non-Connected Standby PV Release

October 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

§

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)
- PV 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 8.1 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
- Spread Spectrum Clocking percentage (SSC%) adjustment has been added to this release's FITC version, in SOC Strap 3. Refer to the Bring Up guide for more details.

§

4 Issues Fixed

4.1 Firmware

Issue #	Description	Affected Component/Impact / Workaround/Status
216744	FPTw: fail to perform -closemnf on prelock SPI image	**Affected Component:** FPT Tool. **Problem:** Closemnf fails when using Pre Lock SPI image **Root cause:** FPT - WRITEGLOBAL is *required* to be run before closemnf. 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

§