Bay Trail M/D Platform – Intel® Trusted Execution Engine (Intel® TXE) 1.0 FW (3MB & 1.25MB)

Firmware Release Notes

Hot Fix 4 Release

January 2014

Intel Confidential

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

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.

Copyright © 2014, Intel Corporation. All rights reserved.

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	OS Support
FITC	• Flash Image Creation Tool • Provides both a GUI and a command line tool	Windows* 7, Windows* 8, Windows* 8.1
FPT	• Flash Programming Tool • Tools Provided within Windows command line tool.	Windows* 8, Windows* 8.1 EFI Shell, WinPE* 4.0
TXEInfo	• Intel TXE setting checker tool	Windows* 8, Windows* 8.1, EFI Shell, WinPE 4.0
TXEManuf	• Validates Intel TXE functionality on manufacturing line	Windows* 8, Windows* 8.1, EFI Shell, WinPE 4.0
FWUpdate	• Updates the Intel TXE FW code region on a flash device that has already been programmed with a complete SPI image	Windows* 7 64bit, Windows* 8, Windows* 8.1, EFI Shell, WinPE 4.0

2.1.3 Versions

Type	Version
Intel® TXE FW	1.0.4.1089
Intel® TXEI driver	1.0.0.1064

§

3 Important Notes

- Please note: HF2 release is followed by HF4.
- This kit includes both full SKU (3MB Intel TXE FW) and thin SKU (1.25MB Intel TXE FW)
- 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)
- 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.
- 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 1.0.4.1089 Intel TXE FW to ‘4’. As a result, Full FW upgrades from earlier releases are possible. However, a downgrade from 1.0.4.1089 to earlier version is not possible.

§

4 Fixed Issues

4.1 Firmware

Issue #	Description	Description/ Affected Component/ Impact / Status
216687	TXEManuf MicroKernel - Internal Hardware Test failed	**Description:** When using signed PV Intel TXE Firmware with Pre Production Silicon parts, TXEManuf MicroKernel test will fail. **Impact:** TXEManuf.exe operation fails. **Fixed**
216859	Intel TXEI driver yellow bang after S4 Cycling	**Description:** After long run of S4 cycle test, Intel TXEI driver shows yellow bang **Impact:** No communication with Intel TXE in OS **Fixed**
5017320	Intel TXE 1.25/3M version cannot be updated via FWUpdate randomly.	**Description:** Error message appear randomly "Intel Txe Interface : cannot locate TXE device" upon using FWUpdate tool **Impact:** FWUpdate tool functionality **Fixed**

§