



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

Firmware Release Notes

Windows* 7 64-bit Beta Release

December 2013

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 © 2013, Intel Corporation. All rights reserved.



Contents

1	Introduction	4
1.1	Scope of Document	4
1.2	Acronyms.....	4
2	Release Kit Summary	5
2.1	Contents of Downloaded Kit.....	5
2.1.1	Documents.....	5
2.1.2	Tools	6
2.1.3	Versions.....	6
3	Important Notes	7
4	Known Issues	8
4.1	Firmware	8

§



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 Intel® Pentium® processor or 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

Tool	Description	OS Support
FITC	<ul style="list-style-type: none"> • Flash Image Creation Tool • Provides both a GUI and a command line tool 	Windows* 7, Windows* 8, Windows* 8.1 64bit
FPT	<ul style="list-style-type: none"> • Flash Programming Tool • Tools Provided within Windows command line tool. 	Windows* 8, Windows* 8.1 64bit, EFI Shell, Windows* PE 4.0
TXEInfo	<ul style="list-style-type: none"> • Intel TXE setting checker tool 	Windows* 8, Windows* 8.1 64bit, EFI Shell, Windows* PE 4.0
TXEManuf	<ul style="list-style-type: none"> • Validates Intel TXE functionality on manufacturing line 	Windows* 8, Windows* 8.1 64bit, EFI Shell, Windows* PE 4.0
FWUpdate	<ul style="list-style-type: none"> • 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 64bit, EFI Shell, Windows* PE 4.0



2.1.2 Tools

Note: FPT, TXEInfo, TXEManuf tools do not support Windows 7. Customer requested to run Intel TXE manufacturing tools in EFI Shell or Windows PE (WinPE) environment.

2.1.3 Versions

Type	Version
Intel® TXE FW	1.0.2.1060
Intel® TXE System Tools	1.0.2.1065
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)
- Windows 7 Beta kit supports the following:
 - Booting with Intel TXE Enabled
 - Intel TXE System Tools (Please refer to section 2.1.2 for OS support)
 - 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.
- BIOS release notes are part of the Bay Trail M/D platform, Bayley Bay - Customer Reference Board BIOS Image kit
- Please note that this kit is aligned with Bay Trail-M/D Platform Windows 7 64 Bit Beta Best Known Configuration
- FPT, TXEInfo, TXEManuf tools do not support Windows 7. Customer requested to run Intel TXE manufacturing tools in EFI Shell or Windows PE environment.

§



4 Known Issues

4.1 Firmware

Issue #	Description	Affected Component/Impact / Workaround/Status
NA	A yellow bang appears on Intel® TXEI device upon installation of Intel TXEI driver in Windows 7	Affected Component: Intel® TXEI Driver Root cause: TXEI Driver uses KMDF (WDF) 1.11, which is built-in Windows 8 and Windows 8.1. However, Windows 7 doesn't have it Resolution: Please install Kernel-Mode Driver Framework (KMDF) version 1.1. Please follow instructions in this link: KB2685811