



# **Bay Trail M/D Platform – Intel<sup>®</sup> Trusted Execution Engine (Intel<sup>®</sup> TXE) FW**

**Firmware Release Notes**

---

*Single Intel<sup>®</sup> TXE FW for Android\* based UEFI BIOS and  
Windows\* 8.1 32-bit - Alpha Release*

*November 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>

This document contains information on products in the design phase of development.

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, Intel Insider, 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 Intel® TXE 1.1 FW Feature Overview .....	4
	1.2 Acronyms.....	5
	1.3 Reference Documents .....	5
2	Release Kit Summary .....	6
	2.1 Contents of Downloaded Kit .....	6
	2.1.1 Documents.....	6
	2.1.2 Tools .....	6
	2.1.3 Versions.....	6
3	Important Notes .....	7



# 1 Introduction

Intel® Trusted Execution Engine (Intel® TXE) Firmware 1.1 SKU introduces single Intel TXE FW that supports both Android\* based UEFI BIOS and Windows\* 8.1 32-bit.

Intel TXE collaterals have been updated accordingly (See chapter 1.3)

This document provides component level details of the downloaded kit.

## 1.1 Intel® TXE 1.1 FW Feature Overview

Intel® TXE FW Feature	Windows* 8 32-bit & 64-bit; Windows* 8.1 64 bit - Major SKU (3MB)	Windows* 8 64-bit; Windows* 8.1 64-bit - Thin SKU (1.25MB)	Android* based UEFI BIOS and Windows* 8.1 32-bit - (3MB)
Widevine*	No	No	Yes
Miracast	No	No	Yes
Protected Audio Video Path (PAVP)	Yes	No	Yes
Field Programmable Fuse (FPF)	Yes	Yes	Yes
Intel® TXE Verified Boot	No	No	Yes <sup>1</sup>
Intel® Platform Trust Technology (PTT)	No	No	No
Intel® Insider™	No	No	No
Intel® Identity Protection Technology (IPT)	No	No	No
Intel® Anti-Theft Technology (Intel® AT)	No	No	No
Near Field Communication (NFC)	No	No	No
Intel® Active Management Technology (Intel® AMT)	No	No	No

**NOTE:** <sup>1</sup> Intel® TXE Verified Boot is still being investigated. Further update and documentation will be provided post Alpha.



## 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

## 1.3 Reference Documents

Document	Document no./ Location
Bay trail M/D Platform, Intel® Trusted Execution Engine (Intel® TXE) Firmware. UEFI Android* Manufacturing - Delta from Windows*	CDI / IBL: 538536
Bay Trail-M/D Platform - Intel® Trusted Execution Engine (Intel® TXE) Firmware Compliance Rev2.2	CDI / IBL: 522481
Bay Trail-M/D/T SoC - System Tools for Intel® Trusted Execution Engine Firmware User Guide Rev1.3	Part of Intel TXE FW kit
Bay Trail-MD Intel(R) TXE FW Bring Up Guide Rev1.3	Part of Intel TXE FW kit



## 2 Release Kit Summary

---

This document covers the following Intel® Trusted Execution Engine (Intel® TXE) Firmware release notes for the 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
FPT	Flash Programming 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

Please refer to Android UEFI Board Support Package Release Notes for the full BKC.

Type	Version	Location
Intel® TXE FW	1.1.0.1073	Intel® TXE FW kit - VIP
Intel® TXEI driver	1.0.0.1050	Intel® TXE FW kit - VIP
CRB UEFI BIOS image	V65_32	CDI / IBL
Android OS	Android-4.2.2_r1, Jelly Bean (JB) MR1.1	WW43 BSP on External Server



## 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)
- **Intel® TXE FW Alpha kit for Android based UEFI BIOS supports the following:**
  - Single Intel TXE FW that supports both Android based UEFI BIOS and Windows\* 8.1 32bit with Intel TXE Enabled
  - Widevine provisioning with Windows\*/Windows\* PE and EFI System Tools
  - Intel® Trusted Execution Engine Interface (Intel® TXEI) driver installer – for Windows\* 8.1 32 bit only
- **Intel TXE FW Alpha kit for Android based UEFI BIOS does not support the following: (will be provided post Alpha)**
  - Android OS System tools
  - Create encrypted CEK for Widevine provisioning using certificate provided by Intel
  - Intel® TXE Verified boot feature
- Please note that Intel® TXEI driver for Android OS is provided as part of the Android based UEFI BIOS OS image.

§