



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

Firmware Release Notes

---

*Intel<sup>®</sup> TXE FW 1.1.0.1089 Production Version Point Release  
for Windows\* and UEFI based Android\**

*February 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>

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

No computer system can provide absolute security. Requires an enabled Intel® processor, enabled chipset, firmware, software and may require a subscription with a capable service provider (may not be available in all countries). Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. Consult your system or service provider for availability and functionality.

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, 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 © 2014, Intel Corporation. All rights reserved.



# Contents

---

1	Introduction .....	4
	1.1 Acronyms .....	4
	1.2 Reference Documents/Kits .....	4
2	Release Kit Summary .....	5
	2.1 Contents of Downloaded Kit .....	5
	2.1.1 Documents .....	5
	2.1.2 Tools .....	5
	2.1.3 Versions .....	6
3	Important Notes .....	7
4	Known Issues .....	9
	4.1 Firmware .....	9

§



# 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\*

This document provides component level details of the downloaded kit.

## 1.1 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 (Intel® TXEI)

## 1.2 Reference Documents/Kits

Document	Document no./ Location
Bay Trail-M/D Platform - Intel® Trusted Execution Engine (Intel® TXE) Firmware Compliance Rev2.4	CDI / IBL: 522481
Sample Signer Tool Reference Code	Test Software Collateral ID: <a href="#">1000653</a>
Intel® Trusted Execution Engine (Intel® TXE) Firmware Verified Boot Solution	CDI/ IBL#543127



## 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	<ul style="list-style-type: none"> <li>Flash Image Creation Tool</li> <li>Provides both a GUI and a command line tool</li> </ul>	Windows* 7, Windows* 8, Windows* 8.1 64bit
FLAMInGO	<ul style="list-style-type: none"> <li>Flash Manifest Generation Tool</li> </ul>	Windows* 8, Windows* 8.1 64bit
Sample Signer	<ul style="list-style-type: none"> <li>Flash Manifest Signing Sample Tool</li> </ul>	Windows* 8, Windows* 8.1 64bit
FPT	<ul style="list-style-type: none"> <li>Flash Programming Tool</li> <li>Tools Provided within Windows command line tool.</li> </ul>	Windows* 8, Windows* 8.1 64bit, EFI Shell, WinPE* 4.0
TXEInfo	<ul style="list-style-type: none"> <li>Intel TXE setting checker tool</li> </ul>	Windows* 8, Windows* 8.1 64bit, EFI Shell, WinPE 4.0
TXEManuf	<ul style="list-style-type: none"> <li>Validates Intel TXE functionality on manufacturing line</li> </ul>	Windows* 8, Windows* 8.1 64bit, EFI Shell, WinPE 4.0



Tool	Description	OS Support
FWUpdate	<ul style="list-style-type: none"><li>Updates the Intel TXE FW code region on a flash device that has already been programmed with a complete SPI image</li></ul>	Windows* 7 64bit, Windows* 8, Windows* 8.1 64bit, EFI Shell, WinPE 4.0

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

### 2.1.3 Versions

Type	Version	Location
Intel® TXE FW	1.1.0.1089	Intel® TXE FW kit – VIP
Intel® TXEI driver	1.1.0.1064	Intel® TXE FW kit – VIP

§



## 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)
- Please note that Intel® TXEI driver for Android OS is provided as part of the Android based UEFI BIOS OS image.
- FPT, TXEInfo, TXEManuf tools do not support Windows 7. Customer requested to run TXE manufacturing tools in EFI Shell or WinPE environment.
- For Windows 7 OS only: Intel TXEI Driver uses KMDF (WDF) 1.11, which is built-in on Windows 8 and Windows 8.1. However, Windows 7 doesn't have it. Please install Kernel-Mode Driver Framework (KMDF) version 1.1. Otherwise, yellow bang appears on Intel TXEI device upon installation. Please follow instructions in this link: [KB2685811](#)
- Sample Signer tool reference code kit details available in section 1.2.

**Disclaimer:** SAMPLE SIGNER REFERENCE CODE DOES NOT OFFER ADEQUATE SECURITY. CUSTOMER NEEDS TO ADD SIGNIFICANT FUNCTIONALITY AND MODIFY THIS SOFTWARE TO PROTECT CUSTOMER PRIVATE KEY. INTEL ASSUMES NO LIABILITY FOR LOST OR STOLEN PRIVATE KEY DATA AND/OR SYSTEMS OR ANY OTHER DAMAGES RESULTING THEREOF.





# 4 Known Issues

---

## 4.1 Firmware

Issue #	Description	Description/ Affected Component/ Impact / Status
NA	Intel TXEI installer exe file shows "1.0.0.1064" version in file properties under details tab	<b>Description:</b> Intel TXEI installer exe file shows "1.0.0.1064" version in file properties under details tab. The correct Intel TXEI driver version is 1.1.0.1064 as it is shown in device manager upon installing the driver. <b>Issue will be fixed in next version.</b>