Intel® Trusted Execution Engine (Intel® TXE) 1.1 FW

Intel® TXE FW 1.1.0.1089 Production Version Point Release Update for Windows* and UEFI based Android*

Customer Communication

WW08, February 2014

Legal Disclaimer

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

All 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.

All products, computer systems, dates and figures specified are preliminary based on current expectations, and are subject to change without notice.

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.

Intel, Pentium, Celeron. 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.

Other names and brands may be claimed as the property of others.
All products, computer systems, dates and figures specified are preliminary based on current expectations, and are subject to change without notice.

Table of Contents

Intel® Trusted Execution Engine 1.1.0.1089 Firmware Point Release Update - General Notes

- Intel® Trusted Execution Engine (Intel® TXE) 1.1.0.1089 Firmware Production Version Point Release Update is posted to Intel® VIP
  - ✓ Kit # 100885
- Intel TXE 1.1 FW size is compressed to 1.375MB
- OS Support:
  - ✓ Android* Jelly Bean 32bit[1]
  - ✓ Android Kit Kat 64bit
  - ✓ Windows* 8 32bit & 64bit
  - ✓ Windows 8.1 32bit & 64bit
  - ✓ Windows 7 64bit[1]
- Customers requested to begin using the Intel TXE 1.1 FW point release in manufacturing as soon as possible
  - ✓ No Intel TXE FW update support for update from Intel TXE 1.0 FW (3MB/1.25MB) to Intel TXE 1.1 FW (1.375MB)[2]
  - ✓ Intel will keep limited maintenance path for Intel TXE 1.0 FW **critical issues only** for projects launched with Intel TXE 1.0 FW
  - ✓ Intel expects customers to transition to Intel TXE 1.1 FW in conjunction with C0 stepping

[1] see important note 1
[2] see important note 8

Important Notes

1) Please note: Android* Kit Kat 64 bit support in this kit is Alpha quality. Windows* 7 64 bit support in this kit is PV quality

2) Intel® Platform Protection Technology with Platform Trust (Intel® PTT) is not POR for future Intel® Pentium® processor or Intel® Celeron® processor N- & J- Series based platform (formerly Bay Trail-M/D platform)

Since this configuration is not supported, customers are required to make sure Intel PTT is disabled in BIOS following the FRC and Intel TXE BWG instructions preventing end customer access to Intel PTT options through BIOS control.

3) Using EFI System Tools in UEFI Shell.

- Due to Microsoft's 'Mandatory UEFI Shells and related applications' requirement (System.Fundamentals.Firmware.UEFISecureBoot) when running Intel or customer manufacturing utilities in UEFI shell, the customer is required to disable UEFI Secure boot via BIOS setup menu or UEFI variable. If OEM/ODM wants to run specific EFI tool that needs to run with UEFI secure boot, OEM/ODM will sign that EFI tool with their OEM key

Important Notes

4) Intel TXE PV Firmware is signed by Intel

- PV POR configuration is signed Intel TXE FW and Production Silicon
- Signed Intel TXE FW and Pre Production Silicon is supported for development needs only

Combination of unsigned Intel TXE Firmware and Production Silicon is not supported and will result in unexpected behavior

5) For Windows 7 OS only:

Intel® Trusted Execution Engine Interface (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

Important Notes

6) Sample Signer tool reference code kit available in Test Software - Link: 1000653

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.

7) Field Programmable Fuses are write-once, non-volatile memory. When FPFs are committed, the changes are permanent and irreversible. Please refer to Manufacturing Recommendations for full instructions how to fuse and test FPFs

8) No Intel TXE FW update support for update from Intel TXE 1.0 FW (3MB/1.25MB) to Intel TXE 1.1 FW (1.375MB) or vice versa

   No Intel TXE FW update support for update from Intel TXE 1.0 FW 3MB to Intel TXE 1.0 FW 1.25MB or vice versa

   Note: The above is referring to FWUpdate tool. Update using FPT (Flash Programing Tool) before closing manufacturing will work for all combinations

Windows Manufacturing Collaterals

Document	Title	Location/ Doc #
Manufacturing Recommendations	Bay Trail M/D Platform Manufacturing Recommendation for Intel® Trusted Execution Engine (Intel® TXE) 1.0 SKU Firmware for HR'13 Windows based platform	CDI/IBL: 526064
MAS	Manufacturing Test with Intel® Trusted Execution Engine (Intel® TXE) Firmware on Bay Trail - D/M Windows* OS Platforms	CDI/IBL: 537301

Android* Manufacturing Collaterals

Document	Title	Location / Doc #
Widevine* Keybox Provisioning Training	Bay trail M/D Platform, Intel® Trusted Execution Engine (Intel® TXE) Firmware - Android* Based UEFI BIOS Manufacturing for SR'14 – Widevine* Keybox Provisioning	CDI/IBL: 538536
Manufacturing Recommendations	Bay Trail M/D Platform, Manufacturing Recommendation for Intel® Trusted Execution Engine (Intel® TXE) 1.1 SKU Firmware for SR'14 UEFI Android Platform	CDI/IBL: 541110
MAS	Manufacturing Test with Intel® Trusted Execution Engine (Intel® TXE) on Bay Trail M/D Platforms using Android* OS	CDI/IBL: 541876

Bay Trail-M/D Intel® TXE Compliance Kit

What is the Intel Platform Compliance Kit?

A single kit with multiple tools for Bay Trail-M/D Compliance testing:

- OEMs are requested to test/verify/confirm various Intel® TXE FW compliance tests with these tools
- Tools for debugging (Intel® System Scope Tool)

Each major milestone release will include:

- Intel® Platform Enablement Test Suite (Intel® PETS), Intel® Automated Power Switch (Intel® APS), Intel® System Scope Tool (Intel® SST), and other tools to be included
- User Guides, Compliance Test Results, Release notes and latest Compliance Guide

The Bay Trail-M/D Intel TXE PV Compliance Kit release is available in Test Software - Link : 1000809

- Please Note: There is an update to the Intel TXE Compliance Guide Rev2.4 Doc id: 522481

Intel® Trusted Execution Engine SKUs

Intel® TXE SKU	Intel® TXE 1.0 Full SKU	Intel® TXE 1.0 Thin SKU	Intel® TXE 1.1 PR
Size	3MB	1.25MB	1.375MB
OS Support	Windows only	Windows only	Windows & Android
Last kit version	1.0.4.1089	1.0.4.1089	1.1.0.1089
Feature List			
Widevine*	No	No	Yes
HDCP 2.2	Yes	No	Yes
Protected Audio Video Path (PAVP)	Yes	No	Yes
Field Programmable Fuse (FPF)	Yes	Yes	Yes
Intel® TXE Verified Boot	No	No	Yes
Intel® Platform Protection Technology with Platform Trust (Intel® PTT)	No	No	No
Intel® Insider™	No	No	No
Intel® Identity Protection Technology (Intel® IPT)	No	No	No
Intel® Anti-Theft Technology (Intel® AT)	No	No	No
Near Field Communication (NFC)	No	No	No

Q&A

Q1: Will Intel TXE 1.1 operate with B2 and B3 Bay Trail-M/D stepping?

A1: Yes, Intel TXE 1.1 is supported on all Bay Trail-M/D steppings.

Q2: How long will critical issues support only of Intel TXE 1.0 be available?

A2: Intel recommends customers transition to Intel TXE 1.1 as soon as possible with the features and benefits Intel TXE 1.1 provides. Intel will decrease focus on Intel TXE 1.0 support after C0 production. Intel TXE 1.0 critical issues only support will be at the discretion of Intel after C0 production.