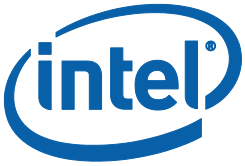

Bay Trail M/D Platform – Intel® Trusted Execution Engine (Intel® TXE) FW

Firmware Release Notes

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

February 2014

Intel Confidential

Contents

§

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: 1000653
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	• Flash Image Creation Tool • Provides both a GUI and a command line tool	Windows* 7, Windows* 8, Windows* 8.1 64bit
FLAMInGO	• Flash Manifest Generation Tool	Windows* 8, Windows* 8.1 64bit
Sample Signer	• Flash Manifest Signing Sample Tool	Windows* 8, Windows* 8.1 64bit
FPT	• Flash Programming Tool • Tools Provided within Windows command line tool.	Windows* 8, Windows* 8.1 64bit, EFI Shell, WinPE* 4.0
TXEInfo	• Intel TXE setting checker tool	Windows* 8, Windows* 8.1 64bit, EFI Shell, WinPE 4.0
TXEManuf	• Validates Intel TXE functionality on manufacturing line	Windows* 8, Windows* 8.1 64bit, EFI Shell, WinPE 4.0

Tool	Description	OS Support
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 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	**Description:** 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. **Issue will be fixed in next version.**