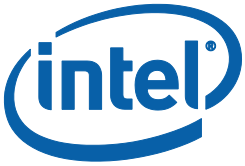

Bay Trail M/D Platform – Intel® Trusted Execution Engine (Intel® TXE) FW

Firmware Release Notes

Single Intel® TXE FW for Android* based UEFI BIOS and Windows* 8.1 32-bit - Alpha Release

November 2013

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* 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[1]
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: [1] 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.

§