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.