



# Braswell - Intel® Trusted Execution Engine (Intel® TXE) 2.0 Firmware

## Intel® TXE FW 2.0.4.3098 Hotfix 4 Release for Windows\* 7, 8.1 & 10 64/32-Bit & Linux

Customer Communication

WW50, Dec 2015



# 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.

Copyright© 2012-2015, Intel Corporation. All rights reserved

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

- General Overview
- Important notes
- Intel® TXE Kit Contents

# Intel® Trusted Execution Engine (Intel® TXE) 2.0.4.3098 HF release - General Overview

- Intel® Trusted Execution Engine (Intel® TXE) 2.0.4.3098 Firmware HF4.
- **New Intel® TXEI Driver 2.0.0.1094** - Certified and digitally signed by the Microsoft\* company.
- This release is posted to Intel® VIP – Kit #112478
- Intel® TXE 2.0 FW size is 1.375MB.
- Supported Operating System:
  - Windows\* 7, 8.1,10 32/64-bit
  - Linux

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.

# HDCP2 RCR Implementation

This release includes a fix for PAVP FW module encryption activation needed to allow Intel to meet HDCP2 license requirements.

## **HDCP2 RX: Encrypting SEC FW**

Encrypting this module is mandatory for meeting HDCP2 license requirements in the situation where Intel distributes CSE FW to OEMs that are HDCP2 licensees.

# TXEInfo Bug

## Background

The latest release of Intel® TXE FW Kit (Version 2.0.2.2092, VIP Kit #111311) introduced a bug in the TXEInfo tool which results in the tool returning an error.

## Error Details

'Error 460: failed getting FPF "Anti Replay Protection FPF" entry from FPF Support Table'

**Reproducibility:** Sporadic

**Affected OSs:** All

## Clarification:

- This error is a TXEInfo tool SW bug **only** and not related to Intel® TXE FW.
- There is no need to update the Intel® TXE FW or the Intel® TXEI driver in order to overcome this issue.

# VCN Version Increase

The VCN (Version Control Number) value has increased in Intel® TXE FW version 2.0.0.2073 (PV Version) to '5'.

As a result downgrades from Intel® TXE FW Version 2.0.4.3098 to earlier Intel® TXE FW versions will not be possible.

Full Intel® TXE FW updates from earlier releases to version 2.0.4.3098 are supported.

# Important Notes

The Intel® TXEI Driver was updated in the previous release following a critical fix in the driver software.

Intel strongly recommends that all customers adopt the below components as published in this kit:

- Intel® TXE FW version 2.0.4.3098
- Intel® TXEI Driver version 2.0.0.1094

Customers who previously targeted the Intel® TXEI driver for Windows\* 10 Update will be required to re-target the driver with the new MSFT Submission ID (SID):

Program	Driver Version	Hardware IDs	Device name	Submission IDs	Operating Systems
Braswell	2.0.0.1094	PCI\VEN_8086&DEV_2298	Intel® TXEI NonRTD3 32-bit	1768789	Windows 7, 8.1, 10 x32
			Intel® TXEI NonRTD3 64-bit	1768790	Windows 7, 8.1, 10 x64

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.

# Important Notes – cont'd

This release contains two versions of the Intel® TXE PV Firmware:

- Production version which is signed by Intel, will run on QS Silicon.
- Pre-production version which is unsigned.

PV firmware is intended for full system integration testing, with all POR features, all platform configurations supported, and all POR operating systems.

# Important Notes – cont'd

PV POR configuration is either one of the following:

- Signed Intel® TXE FW and Production Silicon.
- Unsigned Intel® TXE FW and Pre-Production Silicon.

## Notes:

- In this kit, Unsigned Pre-Production Intel® TXE FW is provided for Development and Testing needs with Pre Production Silicon.
- For Manufacturing and Mass Production purposes Signed Intel® TXE FW and Production Silicon are the only valid combination.

**Combination of Unsigned Intel® TXE Firmware and Production Silicon is not supported and will result in unexpected behavior.**

# Field Programmable Fuses – Manufacturing Flow

- Field Programmable Fuses are write-once, non-volatile memory.
- Once FPFs are committed, the changes are permanent and irreversible.
- FPF values should be committed at EOM using the command: FPT – WRITEGLOBAL before closing manufacturing.
- FPT – CLOSEMNF command will fail if FPT – WRITEGLOBAL was not committed.

# Intel® TXE FW Kit 2.0.4.3098 - Contents

## Software:

- TXE FW Version 2.0.4.3098
- TXEI driver - version 2.0.0.1094
- MUP.xml - version 2.4.3
- TXEI.cat
- TXEI.inf

## System Tools:

- Flash Image Tool - version 2.0.4.3098
- Flash Programming Tool - version 2.0.4.3098
- TXEInfo - version 2.0.4.3098
- TXEManuf - version 2.0.4.3098
- FWUpdate – version 2.0.4.3098
- Flash Manifest Generation Tool 2.0.0.1059
- Sample Signer – version 2.0.0.1059

## Documents:

- Braswell Intel® TXE FW Bring Up guide – rev1.3
- System Tools User Guide – rev 1.2
- FpFConfigurationFile
- Intel(R) TXE FW 2.0.4.3098 Release Notes
- VSCCommn\_bin Content
- HF4 Release Customer Communication

