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

Intel® TXE FW 2.0.0.2073 PV Release for Windows* 7, 8.1 & 10 64-Bit & Linux

Customer Communication

WW28, July 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.

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 (Intel® TXE) 2.0.0.2073 PV release - General Overview

- Intel® Trusted Execution Engine (Intel® TXE) 2.0.0.2073 Firmware PV version for Windows* 7, 8.1 & 10 and Linux.

  This release is posted to Intel® VIP

  - ✓ Kit # 107965

- Intel TXE 2.0 FW size is 1.375MB.

- Supported Operating System:
  - Windows* 7 64-bit
  - Windows* 8.1 32/64-bit
  - Windows* 10 32/64-bit
  - Linux

TXEI Driver Certification:

TXEI Driver 2.0.0.1067 in this PV release was certified and digitally signed by the Microsoft* company.

TXEInfo Error Fix

Problem Description:

Following efficiency measures taken in Intel TXE FW of PC version 2.0.0.2073 for Windows*10 PC release, some redundant FPF table entries were removed and TXEInfo tool was not updated with their removal.

Implication:

Due to this issue, the PC version of TXEInfo tool returned the following error:

"Error 460: failed getting FPF "OEM_UNIQUE_DEVICe_ID" entry from FPF Support Table"

Solution:

TXEInfo tool was corrected in the PV version of this kit and all System Tool were updated to version 2.0.0.2077. No changes were made in IntelTXE FW between PC and PV releases.

Customers are requested to adopt System Tools version 2.0.0.2077 as published in this PV kit for all manufacturing purposes.

Important Notes

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

The VCN (Version Control Number) value has increased in Intel® TXE FW version 2.0.0.2073 (PV Version) to '3'.

As a result downgrades from Intel® TXE FW Version 2.0.0.2073 to earlier Intel® TXE FW versions will not be possible.

Full Intel® TXE FW updates from earlier releases to version 2.0.0.2073 are supported.

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® IPT EPID provisioning affected by MSFT security advisory for **Windows* 7**

Description:

Microsoft released a security advisory about loading external libraries in **Windows*7** OS. – "The issue is caused by applications passing an insufficiently qualified path when loading an external library".

Link to the article: http://technet.microsoft.com/en-us/security/advisory/2269637

This issue affects Intel® IPT EPID provisioning and therefore OEM are required to install the appropriate patch provided by Microsoft*:

http://support.microsoft.com/kb/2533623?wa=wsignin1.0

Intel® TXE FW Kit 2.0.0.2073 - Contents

Software:

- Intel TXE FW Version 2.0.0.2073
- Intel TXEI driver - version 2.0.0.1067
- MUP.xml - version 2.4.3
- TXEI.cat
- TXEI.inf

System Tools:

- Flash Image Tool - version 2.0.0.2077
- Flash Programming Tool - version 2.0.0.2077
  TXEInfo - version 2.0.0.2077
- TXEManuf - version 2.0.0.2077
- FWUpdate – version 2.0.0.2077
- 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 1.0
- FpFConfigurationFile
- Intel® TXE FW 2.0.0.2073 PV Release Notes
- VSCCommn_bin Content
- PV Release Customer Communication