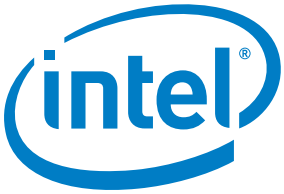

Braswell Platform – Intel® Trusted Execution Engine (Intel® TXE) 2.0 Firmware

Release Notes HF2

19 October 2015

Version History/Revision History

These are the main releases of Braswell FW:

Date	Milestone	Description
Feb 9 2015	Beta	Release Notes for BSW Windows* 8.1 & Windows* 7 **Beta**
Mar 24 2015	PV	Release Notes for BSW Windows* 8.1 & Linux **PV**
Apr 17 2015	Beta	Release Notes for BSW Windows* 10 **Beta**
Apr 21 2015	PV	Release Notes for BSW Windows* 7, 8.1 & Linux **PV**
Jun 26 2015	PC	Release Notes for BSW Windows* 7, 8.1, 10 & Linux **PC**
Jul 09 2015	PV	Release Notes for BSW Windows* 7, 8.1, 10 & Linux **PV**
Jul 23 2015	PV	Release Notes for BSW Windows* 7, 8.1, 10 & Linux **PV**
Jul 27 2015	HF	Release Notes for BSW Windows* 7, 8.1, 10 & Linux **HF**
Aug 27 2015	HF1	Release Notes for BSW Windows* 7, 8.1, 10 & Linux **HF1**
Sept 10 2015	RCR Implementation	Release Notes for BSW Windows* 7, 8.1, 10 & Linux **HF1**
Oct 15th 2015	HF2	Release Notes for BSW Windows* 7, 8.1, 10 & Linux **HF2**

Intended Audience

OEM/ODM software developers, test and validation engineers, system integrators, end-users and or consumers.

Customer Support

For technical support, including answers to questions not addressed in this product, visit the technical support forum, FAQs, and other support information at or contact your Intel Field Application Engineer.

To submit an issue, go to Intel Premier Support:
(https://employeeportal.intel.com/irj/portal/IntelPremierSupportUser)

For more information on registering to Intel Premier Support, go to: http://software.intel.com/en-us/articles/performance-tools-for-software-developers-intel-premier-support

Contents:

1 Introduction

This document covers the following Intel® Trusted Execution Engine (Intel® TXE) 2.0 Firmware Release Notes for future Intel® Pentium® processor or future Intel® Celeron® processor N-series based platform.

Important Notes:

- It is highly recommended to use the FIT tool provided in this kit.
- Please make sure to use Intel TXE FW and System Tools from the same kit. Versioning combinations may cause unexpected issues.
- This kit includes both Unsigned (Pre-production) FW and Signed (Production) FW. Combination of Unsigned Intel TXE Firmware and Production Silicon is not supported and will result in unexpected behavior.
- Please use SPI Flash parts that align with the Braswell Platform SPI Flash Compatibility Requirements (IBL# 550046, section 3)
- Sample Signer tool reference code kit details available in section 5 (Related Documentation).
- The Intel® TXEI driver in this kit has passed the Microsoft* Windows Hardware Quality Labs (WHQL) test and has been certified by the Microsoft* Company.

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.

To learn more about this product, see:

- New features listed in the New in this Release section below, or in the help.
- Reference documentation listed in the Related Documentation section below

2 New in This Release

New Features

- Intel® TXEI Driver version has changed to version 2.0.0.1094 (New MSFT SID #1763523 (x32b), #1763525 (x64b)).
- The VCN (Version Control Number) value has increased in Intel® TXE FW version 2.0.1.2084 (HF1) to '4'. As a result downgrades from Intel® TXE FW Version 2.0.1.2084 to earlier Intel® TXE FW versions will not be possible. Full Intel® TXE FW updates from earlier releases to version 2.0.1.2084 are supported.
- New version of the System Tools User Guide.

Changes to Existing Features

NA

Unsupported or Discontinued Features

As communicated previously, Intel has re-evaluated Android support for Braswell platforms and Android has been removed from the Braswell Plan of Record (POR).

3 Known Issues

Issue #	Title	Description/ Affected Component/ Impact / Status
217378	TXEInfo showing wrong status on last reset reason	**Description**: After issuing global reset, Last Intel® TXE reset reason shows “Power Up” instead of “Global system reset” **Workaround**: Using RW Everything tool, go to Access → "IO Index/Data", Select “0072/0073” index, then locate offset 0x51. Last reset is in bits [7:4] & last reset-1 reset in bits[3:0]. Decode the resets to the following: 0x9 = Warm Reset, 0xB = Cold Reset, 0x2 = Global Reset, 0x0 = Power up.
NA	Intel® IPT EPID provisioning affected by MSFT security advisory for **Windows* 7.**	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 is required to install the appropriate patch provided by Microsoft* : http://support.microsoft.com/kb/2533623?wa=wsignin1.0

4 Fixed Issues

Issue #	Title
RCR 155609	[CHT/BSW] New FPF fuse support by TXE Mfg. Tools for AR disablement
RCR 155600	[CHT/BSW] PTT FW support for configuration with disabled anti-replay protection
N/A	The SetupTXE installer includes a new TCS version 1.42.335.0 with the following changes implemented: ▪ Unified logs location under %PROGRAMDATA%\Intel\iCLS Client ▪ Updated openssl to 1.0.2d version
206070	PR3 bug fix - new enum entry moved in cryprodefs; new pr lib generated.
CL 205687	Fix stack overflow that cause random crash for PlayReady - increase stack size on CHV
1604017961	PlayReady HWDRM content is not playing after resume from sleep.

5 Related Documentation

- Braswell Intel® TXE FW Bring Up Guide
- Braswell Intel® TXE System Tools User Guide
- Braswell Intel® TXE FW Application PRD
- Braswell SPI Programing Guide
- Braswell External Architecture Specification
- Braswell Intel® TXE FW Compliance Guide

Braswell Platform - Intel® Trusted Execution Engine (Intel® TXE) Firmware Compliance – User Guide – Rev. 0.8	CDI / IBL: 554334
Sample Signer Tool Reference Code	Test Software Collateral ID: 1000653
Intel® Trusted Execution Engine (Intel® TXE) Firmware Verified Boot Solution	CDI/IBL: #543127
Braswell Platform SPI Flash Compatibility Requirements	CDI/IBL: #550046
Intel® Trusted Execution Engine HW DRM Playback Failure	CDI/IBL: #561499
Intel® TXE Impact on Platforms Designed without Coin-Cell Batteries	CDI/IBL: #560933

6 Where to Find the Release

This release can be found on the Intel® VIP site: https://platformsw.intel.com

How to Install this Release

This kit can be installed in one of two optional ways:

1. Run SetupTXE.exe located in the Installers sub-directory of the kit.
2. To run silent install, you may use “-s” option as “SetupTXE.exe -s"

7 Release Content

Typical release version numbering is as follows: 2.*x*.*y*.*z* (for example: 2.0.0.zzzz) where:

- '2' refers to the Intel® Trusted Execution 2.x Firmware SKU for Braswell Platforms.
- '*x*' represents point releases where new features or changes to existing features may be added.
- '*y*' refers to Maintenance and Hot Fix release designations.
- '*z*' refers to firmware release revision

Table 1-1 Revision numbers of components of the Production Version release.

Subproject (component)	**Location**	**Revision**
Flash Image Tool (FIT)	…\System Tools\	2.0.2.2092
Flash Programing Tool (FPT)	…\System Tools\	2.0.2.2092
TXEInfo	…\System Tools\	2.0.2.2092
TXEManuf	…\System Tools\	2.0.2.2092
FWUpdate	…\System Tools\	2.0.2.2092
Flash Manifest Generation Tool (FLAMinGO)	…\System Tools\	2.0.0.1059
Sample Signer	…\System Tools\	2.0.0.1059
SetupTXE.exe	…\Installers\	2.0.0.1094

8 Hardware and Software Compatibility

- Intel® Pentium® N3700 Processor
- Intel® Celeron® N3000 Processor
- Intel® Celeron® N3050 Processor
- Intel® Celeron® N3150 Processor

Supported Operating Systems

Windows* 7, Windows* 8.1, Windows* 10, Linux

9 Acronyms and Terms

The following acronyms and terms are used in this document (arranged in alphabetic order):

Acronym/Term	Description
CRB	Customer Reference Board
HECI	Host Embedded Controller Interface
Intel® FIT	Flash Image Tool
FPT	Flash Programming Tool
Intel® TXE	Intel® Trusted Execution Engine (Intel® TXE)
Intel® TXEI	Intel® Trusted Execution Environment Interface (Intel® TXEI)

10 Legal Information

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 This document contains information on products in the design phase of development.Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. Celeron, Intel, the Intel logo, Intel Atom, Intel Inside, the Intel Inside logo, Intel Insider, Look Inside, the Look Inside logo, Pentium, are trademarks of Intel Corporation in the U.S. and/or other countries. *Other names and brands may be claimed as the property of others. Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries. Java is a registered trademark of Oracle and/or its affiliates. Bluetooth is a trademark owned by its proprietor and used by Intel Corporation under license.