

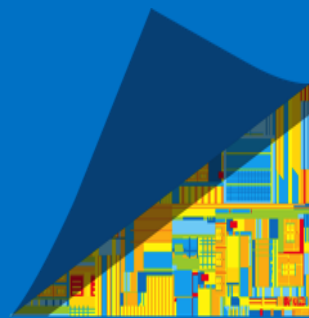


Apollo Lake - Intel® Trusted Execution Engine (Intel® TXE) 3.0 Firmware

Intel® TXE FW 3.0.11.1131 RS1&TH2 HF Release for Windows* 10 64Bit

Customer Communication

WW43 2016



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© 2012-2016, Intel Corporation. All rights reserved

Table of Contents

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

Intel® Trusted Execution Engine (Intel® TXE) 3.0.11.1131 RS1&TH2 HF Release - General Overview

- Intel® Trusted Execution Engine (Intel® TXE) 3.0.11.1131 Firmware RS1&TH2 HF Release.
- This release is posted to Intel® VIP : Kit # **118837**
- Supported Operating System:
 - Windows* 10 64-bit TH2
 - Windows* 10 64-bit RS1

Important Notes

- 1) 3.0.11.1131 Intel® TXE Firmware Kit is supporting B step production Silicon.
- 2) PRQ silicon will boot using Intel® TXE FW Production Version onwards
- 3) This release contains a single version of Intel® TXE Firmware:
 - Production firmware which is signed by Intel production key, will run on B step production Silicon
- 4) Customers are requested to always adopt Intel® TXE FW, Intel® TXE Drivers and Intel® TXE tools versions from the same kit. A mix between kits is not supported and might cause unexpected issues.

Important Notes – Cont'd

5) New features supported:

- NA

Important Notes – Cont'd

6) Secure Tokens functionality:

- Customers that enable Debug Tokens feature **must**
 1. update the Intel® TXE FW to 3.0.2.1108 onwards
 2. Update the OEM key manifest in their image from previous releases using Platform Flash Tool version 5.7.1.0 onwards
 - This change is required due to the public key byte order fix
- Customers will be able to extract the public key hash from the Platform Flash Tool produced signed token **OR** from the private key used to sign the token in Platform Flash Tool
 - Please place the public key hash output inside the OEM Key Manifest under “OemDebugManifest” usage.
- Check Signing & Manifesting Guide on detailed instructions for creating OEM Key Manifest procedure.

Important Notes – Cont'd

7) IFWI Intel required Firmware components include: Intel® TXE, OEM SMIP, CPU uCode patch, PMC FW patch. Please reserve space for the below noted components on SPI per each component maximum size.

- Intel FW fixed SPI size:

Component	Size (KB)
BPDT/SBPDT * 2	2
Descriptor	4
OEM SMIP	16
PMC patch	80
CPU uCode patch	80
Debug Tokens	32
FPF emulation	4
TXE RBE	64
TXE BUP	400
TXE Main	1280
TXE Data (Device Expansion Region)	512
Total	2474

- ISS, iUnit and BIOS sizes are covered in the next slide.

Important Notes – Cont'd

Based on 8MB SPI storage limit, customer BIOS maximum sizes can be increased/decreased according to the configuration choice below:

Intel FW fixed SPI Components (KB) - Mandatory	ISS (Y/N) (260KB) - Optional	iUnit Y/N (40KB) – Optional	BIOS Data Size (KB) – per customer choice*	Max BIOS Size (KB) OBB + IBB - per configuration choice highlighted in green
2474	Y	Y	0	5421
2474	Y	Y	128	5290
2474	Y	Y	256	5162
2474	Y	Y	384	5034
2474	Y	Y	512	4906
2474	Y	N	0	5458
2474	Y	N	128	5330
2474	Y	N	256	5202
2474	Y	N	384	5074
2474	Y	N	512	4946
2474	N	Y	0	5678
2474	N	Y	128	5550
2474	N	Y	256	5422
2474	N	Y	384	5294
2474	N	Y	512	5166
2474	N	N	0	5718
2474	N	N	128	5590
2474	N	N	256	5462
2474	N	N	384	5334
2474	N	N	512	5206

*configured via FIT

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

8) OEM IFWI components signing:

- **For customers that sign the OEM IFWI components:** Signing and Manifesting Guide (part of the Intel TXE kit) includes instructions of how to create OEM Key Manifest and keys relevant for signing various OEM components.
- **For customers that do not sign the OEM IFWI components:** This release supports this option to not sign OEM SMIP, as well as not re-sign the Intel signed ISS, iUnit and Audio FW. Please follow the Signing and Manifesting Guide (part of the Intel TXE kit) instructions

9) Boot Policy Metadata (BPM) creation functionality is available in MEU. Instructions are in Signing and Manifesting Guide

Important Notes – Cont'd

10) In this kit, FPF HW Fusing is supported via FIT for all Field Programmable Fuses, including locking the fuses for end of manufacturing flow which is triggered via **FPT –Closemnf** command. (Refer to MAS documentation for more details, IBL/CDI#: 564139).

Note:

- 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 – Closemnf.
- If customers do not plan to commit the fuses values, please do not trigger FPF –closemnf command on production Silicon with Intel TXE Production FW!

Important Notes – Cont'd

11) In this kit, Intel® TXEI driver is certified by Microsoft (version 3.0.0.1115)

- Note: Intel TXE driver is compliant with Device guard (HVCI)
- The submission id for Intel® TXEI driver version 3.0.0.1115 is : 1880901

12) The VCN (Version Control Number) value has been increased in 3.0.10.1129 Intel® TXE FW (RS1 PV version) to '10'. As a result, Intel® TXE FW upgrades from earlier releases are possible. However, a downgrade from 3.0.10.1129 to earlier version is not possible.

Important Notes – Cont'd

13) Note: IBVs must properly implement all TXE-IAFW(BIOS) interfaces documented in IAFW spec for boot flows and FW capsule update. (CDI/IBL Doc#: 559811)

14) Intel® TXE Compliance Kit QS release is available on VIP –Kit #1012716

ID	Title	Description	Post Date	Collateral Type
<u>1012716</u>	Intel® Trusted Execution Engine Compliance & Debug Kit 3.0.1089.880v2	Engineering Release: Intel® Trusted Execution Engine Compliance and Debug Kit Rev 3.0.1089.880v2 (WW25'16) supporting Intel® TXE Firmware 3.0 QS Engineering Release for Windows* 10 64-bit.	6/15/2016	Test Software

Intel® TXE FW Kit 3.0.11.1131 - Contents

Firmware:

- Intel® TXE FW Version 3.0.11.1131

Software:

- Intel® TXEI installer - version 3.0.11.1131
- MUP.xml - version 2.4.3
- Intel® TXEI driver - version 3.0.0.1115

System Tools:

- Flash Image Tool - version 3.0.11.1131
- Flash Programming Tool - version 3.0.11.1131
- TXEInfo - version 3.0.11.1131
- TXEManuf - version 3.0.11.1131
- Manifest Extension Utility – version 3.0.11.1131
- Platform Flash Tool – version 5.8.0.0

Documents:

- Intel® TXE FW Bring Up guide – rev1.1
- System Tools User Guide – rev1.0
- Signing and manifesting guide – rev1.1
- Secure Tokens Guide rev 1.0
- SMIP and SPI programming guide – rev1.0
- VSCCommn_bin Content
- Intel® TXE FW 3.0.11.1131 Release Notes
- Intel® TXE FW 3.0.11.1131 RS1&TH2 HF Release Customer Communication

