Intel® Trusted Execution Engine (Intel® TXE) 1.0 Firmware

Intel® TXE FW 1.0.5.1120 Hot Fix Release for Windows*

Customer Communication

WW38, September 2014

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® Trusted Execution Engine (Intel® TXE) 1.0.5.1120 Hot Fix release - General Overview

- Intel® Trusted Execution Engine (Intel® TXE) 1.0.5.1120 Hot Fix release has been posted on VIP - Kit # 103381. This kit includes the following:
  - TXE FW 3MB SKU
  - TXE FW 1.25MB - Thin SKU
- OS Support:
  - ✓ Windows* 8 32bit & 64bit
  - ✓ Windows 8.1 32bit & 64bit
  - ✓ Windows 7 64bit
- This Hot Fix was released to de-feature the Top-Swap mechanism (see next slide for details).

Top-Swap Update

Problem: Writing the General Control Register may cause the Top Swap mechanism to become incorrectly configured, resulting in unreliable boot behavior which may impact system availability.

Impacted: Baytrail SKUs.

Mitigation Options: Root cause has been determined. Intel has released Intel® TXE Firmware workaround to disable Top Swap for the impacted processors.

Recommendation: Intel recommends customers update the Intel® TXE Firmware at their earliest convenience.

For details refer to Errata **VLP62** in the Intel® Celeron® and Pentium® Processor N- and J- Series Specification Update (CDI/IBL - **534984**)