Intel® Trusted Device Setup (Intel® TDS)

PMT Platform Measurement Tool

Release Notes

Component version: 2.19PV

Release Date: ww43’20

Intel Confidential

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%20>

All products, platforms, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice. All dates specified are target dates, are provided for planning purposes only and are subject to change.

This document contains information on products in the design phase of development. Do not finalize a design with this information. Revised information will be published when the product is available. Verify with your local sales office that you have the latest datasheet before finalizing a design.

Intel® Active Management Technology requires activation and a system with a corporate network connection, an Intel® AMT-enabled chipset, network hardware and software. For notebooks, Intel AMT may be unavailable or limited over a host OS-based VPN, when connecting wirelessly, on battery power, sleeping, hibernating or powered off. Results dependent upon hardware, setup and configuration. For more information, visit [Intel® Active Management Technology](http://www.intel.com/content/www/us/en/architecture-and-technology/intel-active-management-technology.html).

No computer system can provide absolute security. Intel® Identity Protection Technology requires an Intel® Identity Protection Technology-enabled system, including an enabled Intel® processor, enabled chipset, firmware, software, and Intel integrated graphics (in some cases) and participating website/service. Intel assumes no liability for lost or stolen data and/or systems or any resulting damages. For more information, visit <http://ipt.intel.com/>.  Consult your system manufacturer and/or software vendor for more information.

KVM Remote Control (Keyboard, Video, Mouse) is only available with Intel® Core™ i5 vPro™ and Core™ i7 vPro™ processors with Intel® Active Management technology activated and configured and with integrated graphics active. Discrete graphics are not supported.

Intel® vPro™ Technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software and IT environment. To learn more visit: <http://www.intel.com/technology/vpro>.

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.

\*Other names and brands may be claimed as the property of others.

Copyright © 2020, Intel Corporation. All rights reserved.

Contents

[1 General Information 5](#_Toc40783371)

[1.1 Important Notes 5](#_Toc40783372)

[2 PMT Tool List of New Features (RCRs) in this release 6](#_Toc40783373)

[3 Issue Status Definitions 7](#_Toc40783374)

[4 PMT Tool Resolved Issues in this Release 8](#_Toc40783375)

[5 PMT Tool Open/Known Issues 9](#_Toc40783376)

Revision History

|  |  |  |
| --- | --- | --- |
| Revision Date | Revision Number | Description |
| June 25, 2018 | 1.00 | Added functional modules block diagrams in section Alpha Release with final reviews ready for MSFT |
| Oct 25, 2018 | 1.10 | Sealing Key Hash function incorporated for .der and .pem files |
| Dec 10, 2018 | 1.20 | Changes to reflect SAS Ver 0.92 - Product Name and SKU Number length increase to 64 bytes. Seal Configuration added 2 bytes and removed 2 bytes from Reserved |
| Jan 11, 2019 | 1.22 | Changes to reflect SAS Ver. 0.83 - Disk Measurement removing GPT hash and adding the Partition 0 Measurement Type (0, 1,2, 3) adding support for PCR 11. |
| Jan 25, 2019 | 2.00B | **Beta Release** - Added the PMT Binary Integration and Signing module (Integration of the MEU tool) The PMT tool will now perform generation of the Singed GMF binary and signing. |
| Mar 3, 2019 | 2.06B | Added the –winblog to read the TPM PCR values from the windows boot log file |
| Mar 18, 2019 | 2.07B | Changed default to read the PCR Values from the Windows boot log file. Added -tpmpcr option to read the PCR values from the TPM. -winblog is no longer necessary but is still a valid option. |
| July 14, 2019 | 2.08B | Add Hex Dump of TPM Log File in the GETWBCL option, Check PCR5 DC\_Configuration variable for GMFSigningEnabled and MeasurementCollection bits set; Add Disk Measurement Type 3 Existing BOM File; Add seal configuration parameters used by the seal .ini file to the pmt .ini file; ; Log file to initialize PCR [0] to 3 when ACM sends SU from locality 3. |
| July 22, 2019 | 2.09B | PCR [0] locality 3 changed from Big-endian to Little-endian |
| August 21, 2019 | 2.10B | 1) Extra byte bug fixed on pmf.binary PCR hash, 2.) Added the Expiry date checking – PMT will fail if the expiry date is has passed. Changed the “ExpireDate” parameter in pmt.ini to “ExpiryDate”. 3.) Debug flag in the meu manifest header is turned on by default. PMT will look for pmt\_private.pem, pmt\_public.pem & pmt\_certificate.bin at local folder by default if the meu\_pmf\_manifest.xml file is not being used. |
| September 26,2019 | 2.11B | 1) Fixed: “Error during CryptCreateHash” on first run on new system 2) updated OpenSSL Version 1.0.2T Sept 2019 release. 3) PMT tool now checks the PMFSigningEnabled flag in pmf.ini file. 4) PMT tool will automatically scan for all of the partition and then set Partition Measurement Type=0 by default unless the Partition Measurement Type is specified in the pmt.ini file. 5) The pmt.ini file now support comments using # for single line and /\* comment \*/ for commented sections. |
| October 7, 2019 | 2.12B | 1) Fixed the OS Build Number in PMF does not match OS Build Number in SVT. |
| October 9, 2019 | 2.13B | 1) Fixed PMT Tool did not unload the unload “HKEY\_LOCAL\_MACHINE\WIN10\_REG\_SOFTWARE” |
| December 3, 2019 | 2.14PV  Production Candidate Release | 1) Removed dependencies on the tbs.dll for the PMT tool to run. Note: If the TPM PCR resisters are read directly from the TPM then tbs.dll is still required.  2) TPM Log File filename is used to read the latest log file entry. Log file naming uses an incremental filename. The log file write date is not used to determine the latest file  3) Added note that spaces are valid characters in PartitionBOMFileName(0,1,2,…)= filenames |
| April 26, 2020 | 2.15PV | 1) When signing the PMF, PMT expects to provide a Certificate for the PMF signing key. The  PMT should restricted the public key to RSA 2048. Version 2.14 checks the Signature Algorithm field which is incorrect. It now checks the Subject Public Key Algorithm Info field |
| May 19, 2020 | 2.16PV | 1) Changed the version output text from 2.15B to 2.16PV. 2) Fixed the PCR [1,4,7,11] & platform measurement error observed while Sealing(From OS) with latest Dropship ‘PMT Tool v2.15’ |
| Oct 7, 2020 | 2.18PV | 1) Changed the version output text from 2.17PV to 2.18PV. 2) fix error on Windows Crypto API call |
| Oct 23, 2020 | 2.19PV | 1) Updated with VS2017. 2) Updated with Openssl 1.1.1h. |

# General Information

## Important Notes

**Scope of the release**

This is the Production release for the Intel® TDS Platform Measurement Tool for customer production.

1. The PMT tool was updated in Ver 2.18PV to fix error on Windows Crypto API call.

|  |  |
| --- | --- |
| **NTE\_KEYSET\_ENTRY\_BAD**  0x8009001AL  The *pszContainer* key container was found but is corrupt. | PMT The error is from the Windows Crypto API where the local key container that created by PMT was corrupted.  Root Cause could be:  - Some other services or tools that are creating the key container with same name as PMT.  - PMT didn’t clear the container properly when it failed at certain point.  Corrective Actions  - PMT Version 2.18PV now has a new container name & close the container properly. |

# PMT Tool List of New Features (RCRs) in this release

| **Change #** | **Change details** |
| --- | --- |
| N/A | N/A |
|  |  |

# Issue Status Definitions

This document provides sightings and bugs report for Intel® TDS PMT Tool.

**Closed/Resolved Issues**: This category will only display closed issues within the current Intel® PMT Tool release. After each release, old issues will be dropped down to the “Archive” section and then new closed issues will take its place back up top for the next release. If an issue is posted in this section, it will indicate that the issue has been verified and fixed within the kit that is being released.

**Known/Open Issues**: This category will display all Known Issues since the Beta release and will remain in this section until fixed or noted otherwise. “Known Issues” are still under investigation and may or may not be root caused.

**Archive – Fixes in Previous Kits**: This category will display all closed issues that were closed in their respected kit#. This section will serve as a history of fixed issues.

# PMT Tool Resolved Issues in this Release

| Issue # | Description | Details | Notes |
| --- | --- | --- | --- |
|  |  |  |  |

# PMT Tool Open/Known Issues

| Issue # | Description | Details | Notes |
| --- | --- | --- | --- |
| None |  |  |  |