Intel® Trusted Platform Module Tools

User Guide | November 2007 | Revision 0.56

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.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

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. This document contains information on products in the design phase of development.

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.

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.

Additional technology disclaimers are found on the Intel intranet:
http://legal.intel.com/Marketing/notices+and+disclaimers

I2C is a two-wire communications bus/protocol developed by Philips. SMBus is a subset of the I2C bus/protocol and was developed by Intel. Implementations of the I2C bus/protocol may require licenses from various entities, including Philips Electronics N.V. and North American Philips Corporation.

Alert on LAN is a result of the Intel-IBM Advanced Manageability Alliance and a trademark of IBM.

Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. See www.intel.com/products/processor_number for details.

Intel® TPM and other 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.

Intel, Intel® AMT and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

Software License Agreement

IMPORTANT—READ BEFORE COPYING, INSTALLING OR USING.
Do not use or load this software or any associated materials (collectively, the "Software") until you have carefully read the following terms and conditions. By loading or using the Software, you agree to the terms of this Agreement. If you do not wish to so agree, do not install or use the Software.

- **LICENSE:** Subject to the restrictions below, Intel Corporation ("Intel") grants you the following limited, revocable, non-exclusive, non-assignable, royalty-free copyright licenses in the Software. The Software may contain the software and other property of third-party suppliers, some of which may be identified in, and licensed in accordance with, the "license.txt" file or other text or file in the Software.
- **DEVELOPER TOOLS:** Including developer documentation, installation or development utilities, and other materials, including documentation. You may use, modify and copy them internally for the purposes of using the Software as herein licensed, but you may not distribute all or any portion of them.
- **RESTRICTIONS:** You will make reasonable efforts to discontinue use of the Software licensed hereunder upon Intel's release of an update, upgrade or new version of the Software. You shall not reverse-assemble, reverse-compile, or otherwise reverse-engineer all or any portion of the Software.

Use of the Software is also subject to the following limitations. You:

- Are solely responsible to your customers for any update or support obligation or other liability which may arise from the distribution of your product(s).
- Shall not make any statement that your product is "certified," or that its performance is guaranteed in any way by Intel.
- Shall not use Intel's name or trademarks to market your product without written permission.
- Shall prohibit disassembly and reverse engineering.
- Shall indemnify, hold harmless, and defend Intel and its suppliers from and against any claims or lawsuits, including attorney's fees, that arise or result from your distribution of any product.

Ownership of Software and Copyrights

Title to all copies of the Software remains with Intel or its suppliers. The Software is copyrighted and protected by the laws of the United States and other countries, and international treaty provisions. You will not remove, alter, deface or obscure any copyright notices in the Software. Intel may make changes to the Software or to items referenced therein at any time without notice, but is not obligated to support or update the Software. Except as otherwise expressly provided, Intel grants no express or implied right under Intel patents, copyrights, trademarks, or other intellectual property rights. You may transfer the Software only if the recipient agrees to be fully bound by these terms and if you retain no copies of the Software.

Limited Media Warranty

If the Software has been delivered by Intel on physical media, Intel warrants the media to be free from material physical defects for a period of ninety (90) days after delivery by Intel. If such a defect is found, return the media to Intel for replacement or alternate delivery of the Software as Intel may select.

Exclusion of Other Warranties

EXCEPT AS PROVIDED ABOVE, THE SOFTWARE IS PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY OF ANY KIND INCLUDING WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. Intel or its suppliers do not warrant or assume responsibility for the accuracy or completeness of any information, text, graphics, links or other items contained in the Software.

Limitation of Liability

IN NO EVENT SHALL INTEL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, OR LOST INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF INTEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS PROHIBIT EXCLUSION OR LIMITATION OF LIABILITY FOR IMPLIED WARRANTIES OR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION.

Table of Contents

Revision History

Date	Revision Number	Modifications
19 Aug 07	0.49	Doc creation
23 Aug 07	0.50	Added iTPMDiag details
16 Aug 2007	0.51	Added OS support
03 Sep 2007	0.52	New format
10 Oct 2007	0.53	Minor corrections
11 Nov 2007	0.56	Name change

1. Introduction

This guide describes the firmware image tools specific to Intel® Trusted Platform Module (Intel® TPM) and their use, as well as a brief description of the general system tools. It also describes tools that are not Intel® TPM-specific but feature Intel® TPM-related functionality.

Terminology

Acronym / Term	Description
AMT	Active Management Technology
BIST	Built-In Self Test
FIT	Flash Image Tool
FPT	Flash Programming Tool
FW	Firmware
GbE	Gigabit Ethernet
TPM	Trusted Platform Module
LMS	Local Manageability Service
MAC	Media Access Control
ME	Manageability Engine
NVM	Non-Volatile Memory
OOB	Out-of-Band
OS	Operating System
SKU	Stock Keeping Unit
SOL	Serial Over LAN
SPI Flash	Serial Peripheral Interface Flash

Sx	Sleep State (where x is the specific state)

Reference Documents

Title	Location / Description
Standard TPM documents	https://www.trustedcomputinggroup.org/specs/TPM Design principles, structures, and command documents within the above link are of use.
Intel® TPM Ordinal Extensions	WIP—will be part of the OEM kit downloadable from the ARMS website.
Intel® ME Systems Tools User Guide	Found as part of the OEM kit downloadable from the ARMS website.
OEM Bringup Guide	Found as part of the OEM kit downloadable from the ARMS website.
Intel® TPM Compliance & Test Guide	WIP—will be part of the OEM kit downloadable from the ARMS website.
AMT Tools User Guide	Found as part of the OEM kit downloadable from the ARMS website.

2. Preface

Intel® Management Engine (ME) Functionality

The ME hardware architecture available in Intel® vPro™ platforms offers several advanced features, such as:

- Intel® Active Management Technology (Intel® AMT) capabilities, including out-of-band (OOB) operation.
- Dedicated memory space within the main memory where ME code may be executed and ME run-time data stored.
- Intel® Quiet System Technology (Intel® QST) providing advanced fan and temperature control for reduced system noise emission.
- Intel® TPM (compliant with TPM 1.2 specification), allowing for trusted platform computing (refer to http://www.trustedcomputinggroup.org).
- A LAN controller that supports Out-of-Band (OOB) activity.

3. Introduction to Software Tools

Overview

The software tools described in this document are designed to assist in creating, qualifying, and verifying the implementation of Intel® TPM technology on a new platform. A brief overview of the non-TPM-specific tools follows.

Image Editing Tools

- **Flash Image Tool (FIT):** Combines the GbE, BIOS, and ME firmware into a single image that can be programmed by the Flash Programming Tool or any third-party flash programming device.
- **Flash Programming Tool (FPT):** Programs the flash device on the ME hardware. This tool can program individual regions or the entire flash device.
- **FWUpdate:** Updates the firmware code of a flash device that has already been programmed with a complete SPI image.
- **EEUpdate:** Updates the Ethernet MAC address after the firmware has been fully programmed.

Manufacturing Line Validation Tools

Manufacturing line validation tools allow for testing of the ME technology during and immediately after the manufacturing process. These tools are written to operate quickly and run on simple operating systems, such as:

- MS-DOS* 6.22
- Windows* 98 DOS
- FreeDOS*

- DRMK DOS*

A Windows version is also written to run on Windows XP (SP1/2) and Windows Vista*.

- **MEManuf and MEManufWin:** Validate ME device functionality on the manufacturing line.

Integration Validation Tools

Integration validation tools are used by system integrators to check and validate various aspects of ME functionality.

- **MEInfo and MEInfoWin:** Query the ME and return information related to items such as BIOS, FW, Intel® TPM, and ME Interface driver versions.
- **iTPMDiag:** Tests the functionality of Intel® TPM and identifies problematic areas.

Requirements

Manufacturing line validation tools run on MS-DOS* 6.22, Windows* 98 DOS, Windows* XP (SP1/2) or Windows Vista*. Integration validation tools run on Windows (Win2K SP4, XP SP1/2, PE, and Vista) or DOS. Note that not all tools run on DOS.

Integration and validation tools that run locally on the ME device require one or more of the following services to be installed, depending on the SKU:

- Intel® AMT Local Manageability Service (LMS)
- Intel® ME Interface (MEI) driver
- Intel® TPM driver for Intel® TPM testing (only on Windows XP*).

4. Intel® Services

Introduction

The Intel® Management and Security Status Application (Intel® Status application) is a program that provides the ability to monitor and report on Intel® Active Management Technology (Intel® AMT) and Intel® Trusted Platform Module (Intel® TPM) services.

- **Execution:** The file PrivacyIconClient.exe is required to run the Intel® Status application and should be copied to the C:\WINDOWS\system32 directory.
- **Startup:** The program can run automatically at startup by adding it to the Startup directory, or manually by executing PrivacyIconClient.exe.
- **System Tray:** Running the program adds a "vPro™" icon to the notification area.

Intel® Management and Security Status Application

To open the Intel Services property sheet, either double-click the icon or right-click it and select Open. To close the property sheet, click Close. This only closes the window; it does not stop the background application, and the icon will remain in the notification area. To exit the application entirely, right-click the notification icon and select Exit.

General Tab

The General tab provides basic status information and recent events for both Intel® AMT and Intel® TPM.

• Event History: Events and their details are displayed in this section. They can be sorted by clicking on the column headers.
• Service Status: Displays the operational status:
  - Intel® AMT: Configured / Unconfigured / Not detected
  - Intel® TPM: Operational / Not detected
• Options: To launch the interface automatically at login, check the "Intel Services will be available next time I log on to Windows" box.
• Help: Tooltips and context help are available via the Help icon or the "View help for this tab" button.

Intel® AMT Tab

Selecting the Intel® AMT tab displays the Active Management Technology properties.

AMT State

• Status: Operational status of Intel® AMT (Configured / Unconfigured / Not detected).
• Mode: The active environment (Enterprise / Small business / Awaiting configuration / Disabled / Not detected).
• Firmware Version: The running version of the Intel® AMT firmware (e.g., 4.0.0.1031).

Advanced Information

• Open Redirection Sessions: Indicates active redirection sessions (e.g., SOL or IDER active/inactive combinations).

• System Defense State: Displays whether System Defense is active (Activated / Not activated).
• WebUI Status: Shows web management availability (Enabled on TLS / Enabled / Not enabled).
• Last Reset Reason: The reason for the last controller reset (Intel AMT remote boot / Normal reboot).
• Extended System Details: Opens a secondary window containing System UUID, MEI Driver, LMS Driver, and Power Policy.
• Network Information: Displays connection details for wired or wireless adapters (Mode, MAC Information, Link Status, IP Information, Configured for Wireless, Controlling the Interface).

Intel® TPM Tab

The Intel® TPM tab details the Trusted Platform Module status:
• Status: Displays the operational state (Operational / Failed / Not detected).
  - Operational states: Operational - Active; Enabled; Owned / Operational - Not active; Not Enabled; Not Owned.
  - Failure reasons: "Flash corrupted", "HW failure", "ME reset", "Unknown".
• TCG Spec Version: Compliant Trusted Computing Group specification version.
• Firmware Version: The current TPM firmware revision.

5. iTPMDiag and Related Tools

Intel® TPM Diagnostic Tool (iTPMDiag)

iTPMDiag is used to test Intel® TPM functionality and isolate hardware/firmware faults. It is designed for both manufacturing-floor validation and field troubleshooting.
The operations performed by iTPMDiag mirror those of running MEManuf –full –amt+tpm. Both tools initiate the Built-In Self-Test (BIST) routine regardless of the TPM's current initialization state.

OS Support

The iTPMDiag tool is qualified to run on Windows Vista* (32/64-bit), Windows XP* SP1/SP2 (32/64-bit), Windows PE* (Vista & XP based), MS-DOS* V6.22, Windows 98* DOS, DRMK DOS* V8.00, and FreeDOS V1.1.32a.

Usage of the Tool

The tool can be executed locally if the Intel® TPM driver is installed. Standard command-line arguments include:
• No parameters: Runs standard diagnostic sweeps.
• --version: Reports the tool version.
• --verbose: Outputs extended debugging logs, including detailed header, tag, ordinal, and status information per executed command.

Actions

iTPMDiag triggers self-tests for all internal TPM modules:
• If the self-test succeeds, it returns TPM_SUCCESS.
• If any component test fails, it returns TPM_FAILEDSELFTEST, placing the module into failure mode.
• If the self-test process has not yet completed when requested, the TPM may run a comprehensive diagnostic and return TPM_NEEDS_SELFTEST.

Intel® TPM Impact on MEInfo

The MEInfo tool retrieves environmental variables and hardware configurations.

Component	TPM Impact	Field Value
Tools version	X	A version string
BIOS version	X	A version string
GbE version	---	A version string
MEBx Version	X	A version string

AMT Netstack version	---	A version string
AMT version	---	A version string
AMT build number	---	A number
Kernel Version	X	A version string
Kernel Build Num	X	A number
Vendor ID	---	A number
Wireless Hardware Version	X	A version string
Link status	---	Link up / Link down
Hardware SKU	X	AMT, ASF, TPM, and combined profiles
Cryptography fuse	X	Enabled / Disabled
Flash protection	X	Enabled / Disabled
Last ME reset reason	X	Power up / Firmware reset / Global system reset
BIOS boot State	X	Pre Boot / In Boot / Post Boot
Configuration state	---	Not started / In process / Completed
Manageability Mode	---	Intel® AMT / ASF / None
User Notification State	---	Enabled / Disabled
Manuf-mode override behavior	X	Disable / Continue
Host MAC Address	X	A MAC address
Wireless MAC address	X	A MAC address
FWU Override Counter	X	(A number) / Always / Never

FWU Override Qualifier	X	Never / Always / Restricted
Local FWUpdate	X	Enabled / Disabled
Secure FWUpdate	X	Enabled / Disabled
MEI Driver version*	---	A version string
LMS version*	---	A version string
UNS version*	---	A version string
Wireless Driver Version*	X	A version string
TPM fuses (MCH/ICH/soft strap)	X	Enabled / Disabled
TPM Vendor ID	X	A version string
TPM SPEC Version	X	A version string
TPM FW Version	X	A version string
TPM FW Build	X	A number
TPM State	X	Operational / Failed state
TPM Operational Mode	X	Active, Enabled, Owned
iTPM – FIPS 140-2	X	False / True
iTPM - Physical presence life time lock flag	X	False / True
iTPM - Physical presence command enabled flag	X	False / True
iTPM - Physical presence HW enabled flag	X	False / True

*Note: Reported only when the respective driver has been installed and loaded on a supported OS.

Appendix C: TPM Errors

According to the TCG main specifications, error codes fall into five distinct brackets:

- Success: 00000000
- Fatal errors: 00000001 - 000003FF
- Vendor-specific fatal errors: 00000400 - 000007FF
- Non-fatal errors: 00000800 - 00000BFF
- Vendor-specific non-fatal errors: 00000C00 - 00000FFF

Up-to-date documentation regarding standard TPM status flags is maintained at http://www.trustedcomputing.com.

TPM—Non-Fatal Errors

Error Number	Error String	Corrective Action / Details
12048	The TPM is too busy to respond to the command immediately, but the command could be resubmitted at a later time.	The TPM may return TPM_Retry for any command at any point.
12049	SelfTestFull has not been run.	Run full self-diagnostic commands.
12050	The TPM is currently executing a full self-test.	Wait for completion and retry command.
12051	The TPM is defending against dictionary attacks and is in a lockout/timeout period.	Wait for the lockout timer to decay before executing.