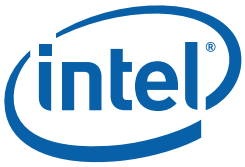


Intel® Active Management Technology (Intel® AMT) 4.0 Firmware Upgrade with Intel® Trusted Platform Module (Intel® TPM)

Whitepaper

June 2008

Revision 0.91

Intel Confidential

Contents

1 Introduction 5

1.1 Purpose and Scope of this Document 5
1.2 Terminology 6
1.3 Reference Materials 7
1.3.1 TCG Specifications 7
1.3.2 TPM Impact on Intel® ME Firmware Update 8

2 Generic Update Procedure for OEM 9

2.1 Downloading and Extracting Upgrades 9
2.1.1 Intel® ME Firmware Upgrade 9
2.1.2 LAN Driver Upgrade 11
2.1.3 BIOS Upgrade 12
2.1.4 File Structure 12
2.2 Performing the Upgrade 12
2.2.1 Intel® ME Firmware Update Command Line 12
2.2.2 BIOS and the LAN driver 13

3 Intel® TPM impact on Intel® ME Firmware Update 15

3.1 Intel® TPM Specification Requirements 15
3.2 Intel® TPM Firmware Update 15
3.3 Impact of TPM State on Firmware Update 16
3.4 Straps and Fuses 17

4 Generic update procedure for End User 19

4.1 Downloading and Extracting Upgrades 19
4.2 Performing the Upgrade 19

5 Appendix A: Bill of Materials (BOM) 21

Figures

Figure 1. High level block diagram of the partitioned HW/SW/FW 9
Figure 2: Search for Kits by Product 10
Figure 3: Typical Cantiga Kits List 10
Figure 4 :Typical Cantiga kit components 11

Tables

Table 1: Optional Arguments for Windows Version of FWUpdate 13
Table 2: AMT-authorized FW update 16
Table 3: Fuse and Strap Description 17
Table 4: Fuse and Strap Configuration 18

Revision History

Revision Number	Description	Revision Date
0.91	Initial release.	June 2008

§

1 Introduction

1.1 Purpose and Scope of this Document

This document is written for the OEM and for the manager of an IT infrastructure. It describes how to perform an Intel® ME Firmware update of existing Intel® Q45 Express Chipset-based Intel® AMT 4.0 clients to the newest Intel® AMT 4.x functionality when the platform has Intel® TPM. This document facilitates the update process with step-by-step instructions, discussion, and troubleshooting tips for the failures that could occur during the update process.

This document applies to the following platforms:

- Mobile Intel® 45 Series Chipset Family (formerly Cantiga) and ICH9M as the lead product in 2008 for Mobile.
- Intel® 4 Series Chipset Family (formerly Eaglelake) and ICH10 in 2008 for desktop.

Support of Intel® ME Firmware update:

- In previous Intel® AMT generations – locally through the HECI, with or without authentication
- For Intel® 45 series chipset family platforms with a discrete TPM – locally through the HECI, with or without authentication
- For Intel® 45 series chipset platforms with Intel® TPM – a modification to support ME firmware updates is required:
    - If the TPM is owned – a TPM Owner pass phrase is required to authorize a ME Firmware update
    - If the TPM is not owned – the policy to authorize a ME Firmware update is executed by ME/MEBx and deferred physical presence, per TCG specification.

References in this document will apply to all 2008 platforms.

This document is intended for the following audiences and purposes:

- OEM can use this procedure to update ME Firmware while manufacturing.
- IT/End-user during field update.
- ME Firmware and BIOS synchronization by OEM.
- Platform applications engineers use this document to support field and customer questions about the product.

1.2 Terminology

Term	Definition
API	Application Programming Interface
ASF	Alert Standard Format
BIOS	Basic Input Output System
BOM	Bill of Materials
Chipset	Combination of ICH & MCH
CPU	Central Processing Unit
DDR2	Double-Data-Rate Two – Synchronous Dynamic Random Access Memory
EFI	Extensible Firmware Interface
FW	Firmware
GbE	Gigabyte Ethernet
gSOAP interface	Communicates with AMT using SOAP on C/C++ web services and clients
GUI	Graphical User Interface
HECI	Host Embedded Controller Interface
HMAC-SHA1	Hash Based Message Authentication Code using SHA1 Hash function based on RFC 2104 and used as specified in the TPM specification
HT	Hyper-Threading Technology (Intel® CPU feature)
HW	Hardware
ICH	IO Controller Hub (aka South Bridge in Intel® Chipsets)
Intel® AMT	Intel® Active Management Technology
Intel® ME	Intel® Management Engine. Microcontroller in MCH which has (but is not limited to) generic capabilities for security and manageability in OS absent state.
Intel® MEBx	Intel® Management Engine BIOS Extension
Intel® QST	Intel® Quiet System Technology – controlling the fans depending on temperature
Intel® TPM	Intel® Trusted Platform Module
Intel® TXT	Intel® Trusted Execution Technology. Formerly code named LaGrande Technology. Hardware extensions to Intel® processors and chipsets that enhance the digital office platform with security capabilities such as measured launch and protected execution.
IT	Information Technology
LAN	Local Area Network
LMS	Local Manageability Service
MCH	Memory Controller Hub (aka North Bridge in Intel Chipsets)
MEFW	Intel® Management Engine Firmware
NVM	Non-Volatile Memory

Term	Definition
OEM	Original Equipment Manufacturer
PC	Personal Computer
PCB	Printed Circuit Board
ROM	Read only memory
SHA-1	Secure Hash Algorithm as defined in FIPS 180-1
SKU	Stock Keeping Unit
SOAP	Simple Object Access Protocol
SPI	Serial Peripheral Interface
SW	Software
TCG	Trusted Computing Group
TCS	TSS Core Services
TIS	TPM Interface Specification
TLS	Transport Layer Security
TPM Application	Any Host Based Software accessing the TPM via the TPM's standard Interface at localities 0-4
TPME	Trusted Platform Module Entity
TSS	TCG Software Stack
VIP	Validation Internet Portal

1.3 Reference Materials

1.3.1 TCG Specifications

Note: The TCG specifications are, at this time, in various phases of revision.

Date or Rev. #	Title	Location / Owner
1.2	TCG Specification Architecture Overview	https://www.trustedcomputinggroup.org/groups/TCG_1_0_Architecture_Overview.pdf
1.2	TPM Specification 1.2 Level 2 Rev 103	https://www.trustedcomputinggroup.org/specs/TPM/
1.2	TCG PC Specific Implementation Specification Version 1.1	https://www.trustedcomputinggroup.org/specs/PCClient/
1.2	TCG PC Client Specific TPM Interface Specification (TIS) Version 1.2 FINAL Revision 1.00	https://www.trustedcomputinggroup.org/specs/PCClient/

Date or Rev. #	Title	Location / Owner
1.2	TCG PC Client Specific Implementation Specification for Conventional BIOS Version 1.20 FINAL Revision 1.00	https://www.trustedcomputinggroup.org/specs/PCClient/
1.2	TCG EFI Platform Specification Version 1.2	https://www.trustedcomputinggroup.org/specs/PCClient/
1.2	TCG EFI Protocol Specification Version 1.2	https://www.trustedcomputinggroup.org/specs/PCClient/
1.2	TPM Software Stack (TSS)	https://www.trustedcomputinggroup.org/specs/TSS/

1.3.2 TPM Impact on Intel® ME Firmware Update

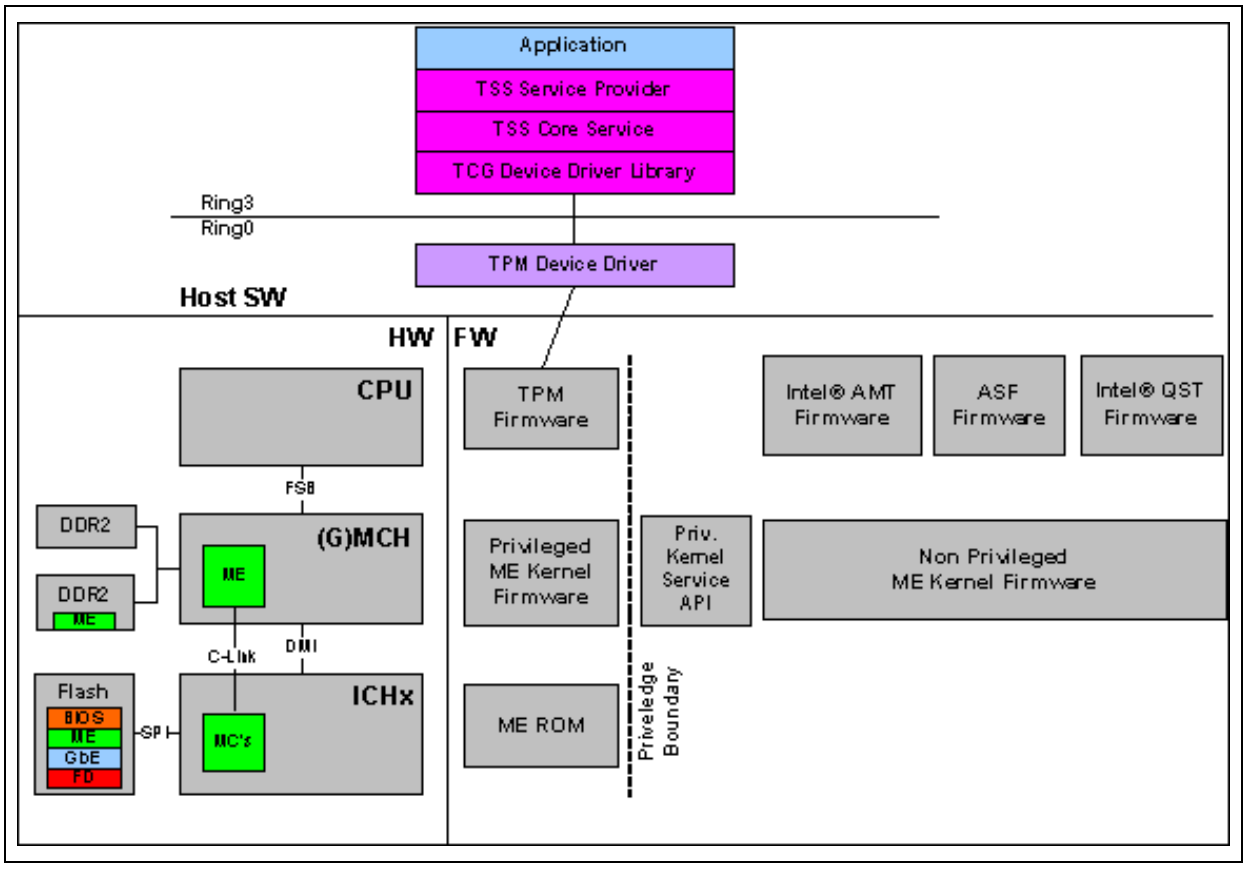
- See Section 9 of the TPM Commands document.
- Details of the **TPM_FieldUpgrade** command may be found here: https://www.trustedcomputinggroup.org/specs/TPM/mainP3Commandsrev103.zip
- For the **TPM_AUTH** details regarding this structure see: https://www.trustedcomputinggroup.org/specs/TPM/mainP2Structrev103.zip
- The **TPM_FieldUpdgrade** ordinal/command may have manufacturer-specific parameters. For details regarding Intel's version of this command, see the Intel® TPM Vendor Specific Ordinals document.

§

2 Generic Update Procedure for OEM

Intel® TPM and Intel® AMT products require the integration of various components, including the Host SW stack, BIOS, ME firmware, and associated HW in the chipset (see Figure 1).

Figure 1. High level block diagram of the partitioned HW/SW/FW



2.1 Downloading and Extracting Upgrades

2.1.1 Intel® ME Firmware Upgrade

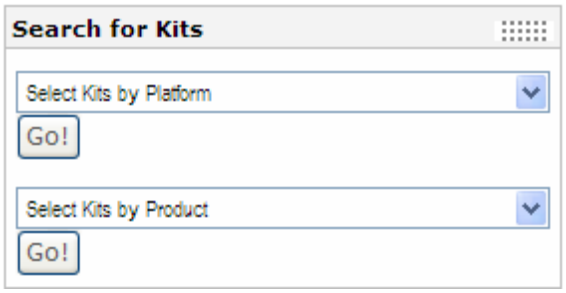
Upgrade clients installed with Intel® AMT release 4.0 will require an ME firmware upgrade to Intel® AMT release 4.x when updating the ME Firmware shared between Intel® AMT and Intel® TPM.

Two files will be necessary to perform the ME Firmware upgrade:

- *FWUpdLcl.exe* – A Windows tool that updates the ME firmware in Flash.
- Binary file containing Intel® AMT release 4.x firmware (to be used by *FWUpdLcl.exe*).

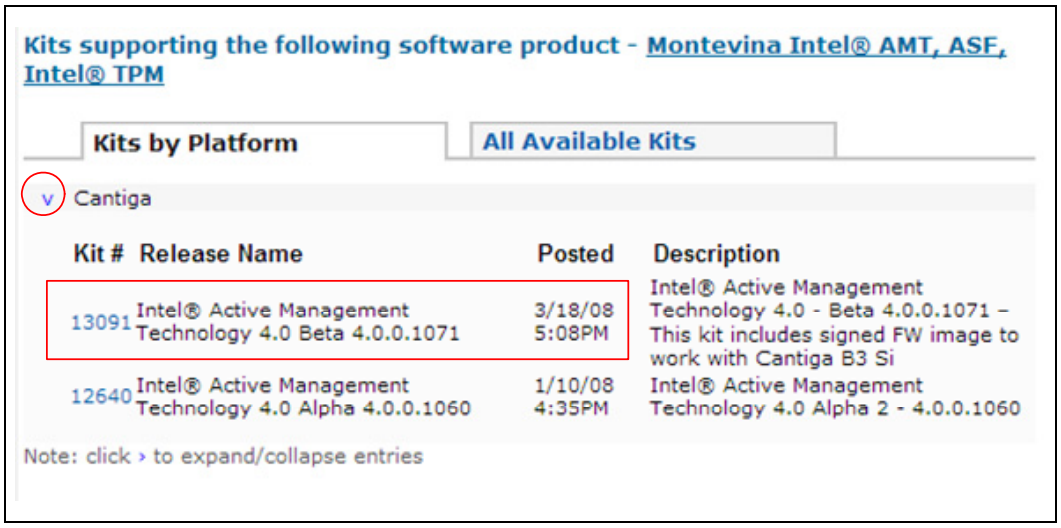
It is necessary to obtain them from Intel in the following way:

1. Use a web browser to navigate to https://platformsw.intel.com/.
2. Enter your username and password into the appropriate fields and click the **Click Here to Log In** button to log into the Intel® Validation Internet Portal.
3. Select *Montevina Intel® AMT, ASF, Intel® TPM* from the **Select Kits by Product** drop-down list in the **Search for Kits** section of the Intel® Validation Internet Portal.
4. Click the **Go!** Button under the **Select Kits by Product** field**.**
5. Click the **>** symbol next to **Cantiga** in the **Kits by Platform** tag to display a list of Cantiga kits.



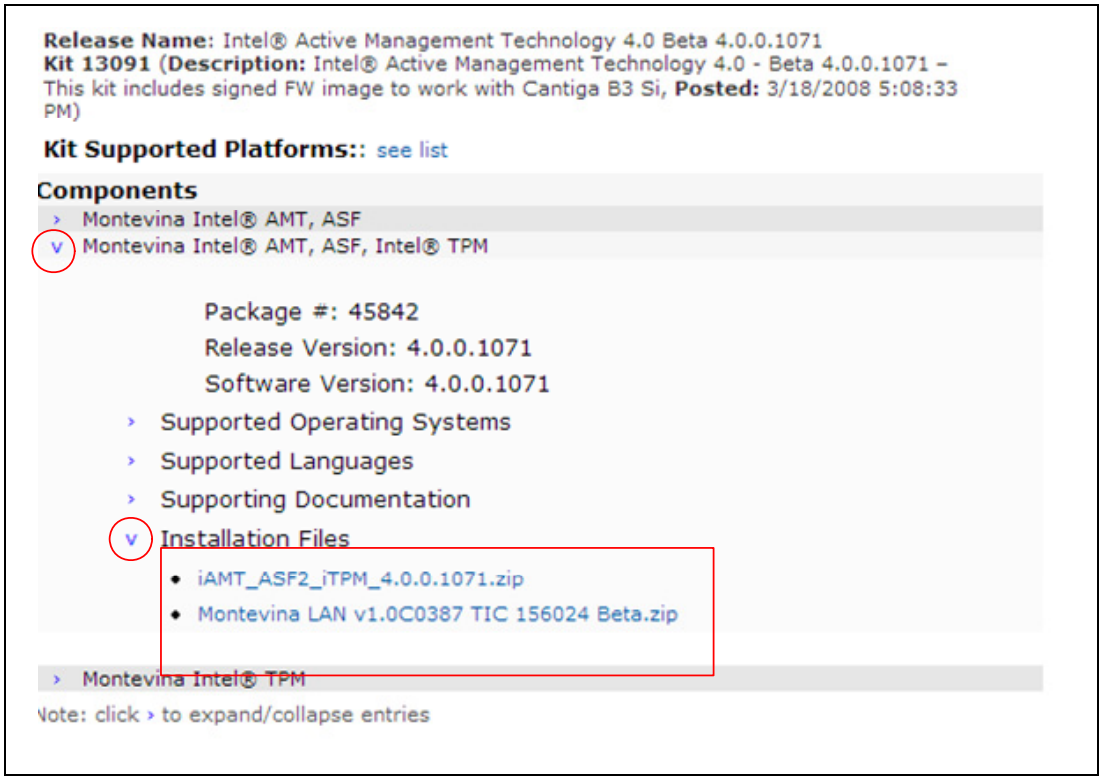
: Search for Kits by Product

Figure 3: Typical Cantiga Kits List



6. Select the version of the Intel® AMT 4.x kit recommended by your computer manufacturer; the screen listing the kit's components appears.
7. Click the > symbols to expand the list of the kit's components until the links to the Installation Files appear (see Figure 4).

Figure 4 :Typical Cantiga kit components



8. Click each of the installation files to start the download process for both of the files.
9. Unzip the contents of the kit file (*iamt_asf2_iTPM_4.x.x.xxxx.zip*) and copy the following two files into a new location (i.e., *C:\AMT41\MEFW*):

   - *\iAMT_ASF2_iTPM_4.1.0.1234\NVM_Image\Firmware\ CA_ICH9_REL_ALL_SKUs_BYP_ME_UPD_Production.BIN*
   - *\iAMT_ASF2_iTPM_4.1.0.1234\System Tools\FWUpdate\Local-Win\FWUpdLcl.exe.*

Note: This document assumes that a kit version 4.x.x.xxxx has been downloaded. Minor and hotfix version values may vary and do not affect this procedure.

2.1.2 LAN Driver Upgrade

A LAN driver upgrade must accompany the Intel® ME firmware upgrade for Intel® AMT release 4.x for clients installed with Intel® AMT release 4.0.

To upgrade the LAN driver:

1. Extract the contents of the EXE archive containing the LAN drivers downloaded from the Intel Validation Internet Portal (see 2.1.1 Intel® ME Firmware Upgrade). (**Note:** This EXE archive is in a ZIP file, so extraction must be performed twice.)
2. Copy the files needed for the BIOS upgrade to the working folder (i.e., *C:\AMT41\LAN*).

2.1.3 BIOS Upgrade

Clients installed with Intel® AMT release 4.0 may also require a BIOS update. A BIOS update package must be obtained from the computer manufacturer. This update package will typically be distributed as an EXE file. The following points must be checked:

- BIOS update package content - if it updates both BIOS and Intel® ME firmware, skip the steps in section 2.1.1 Intel® ME Firmware Upgrade.
- BIOS update package format - if it is an archive (use WinZip* or WinRAR* to verify):
  1. Extract the contents of the archive to a temporary directory.
  2. Copy the files needed for the BIOS upgrade to the working folder (i.e., *C:\AMT41\BIOS*).
  3. Note the name of the BIOS update utility (i.e., *UPDBIOS.exe*).
- BIOS update command line options - the BIOS update must run silently, without requiring any user prompts, and must be executable via the command line. A common way of finding which command line options are available is to run the update utility from the command line using the "**/?**" help switch (i.e., *C:\AMT41\BIOS\UPDBIOS.EXE /?*).

2.1.4 File Structure

The BIOS and Intel® ME Firmware upgrade payload will have the following general structure at this point:

```
C:
└──── AMT41
├──── MEFW
│   ├──── FWUpdLcl.exe
│   └──── CA_ICH9_REL_ALL_SKUs_BYP_ME_UPD_Production.BIN
├──── LAN
│   └──── (LAN driver installation files)
└──── BIOS
├──── UPDBIOS.exe
├──── BIOSIMG.bin
└──── (any other required files)
```

2.2 Performing the Upgrade

2.2.1 Intel® ME Firmware Update Command Line

FWUpdate allows an end user, such as an IT administrator, to update the Intel® ME firmware without having to reprogram the entire Flash device. It then verifies that the update was successful.

FWUpdate does not update the BIOS, GbE, or Descriptor Region. It only updates the portion of the firmware code that Intel provides on the OEM website. FWUpdate will update the entire Intel® ME code area.

The image file that the tool uses for the update is not the image file used to create the complete SPI firmware image file.

A sample firmware image file for updating, *MV_ICH9_REL_IAMT_BYP_ME_UPD.BIN*, is located in the kit's NVM image folder.

Please be aware that firmware update takes approximately 1-4 minutes to complete, based on the Flash device.

FWUpdate is a command line tool and the following data can be input as command line arguments:

- New update image file.
- -TPM – Required if TPM is enabled in the system.
- -verbose – Prints out debug information to the screen

The Windows version of the tool can also receive the optional arguments described in Table 1. These arguments are only relevant for network-based updates (i.e., LMS), and thus only for Intel® AMT machines.

Table 1: Optional Arguments for Windows Version of FWUpdate

Argument	Description
–h	Help
–user <user>	Intel® ME user name for Intel® AMT authorization.
–pass <pass>	Intel® ME password for Intel® AMT authorization.
–eoi	Choose gSOAP interface for Intel® AMT communication.
–tls	Use TLS for communication.
–host <host>	The Intel® AMT host name if TLS is used.
–cert <cert>	Client TLS certificate to use if TLS Mutual authentication is used.
–generic	Perform the update over HECI. Even if the FW supports network update, this will be rejected by the FW if TPM is enabled.
–tpm	Choose TPM interface for the update. **(Note:** -key **or** -msf is mandatory if TPM is in owned state.)
-key <owner_key>	TPM owner password if TPM owned. The TPM owner password must be provided for TPM communication. TPM Passphrase is converted to TPM_AuthData (Owner Authorization), a 160-bit (20 Byte) shared-secret plus high-entropy random number, and passed to TPM_FieldUpdgrade ordinal. The algorithm used to create the TPM_AuthData takes the TPM Passphrase and the random number and mixes them with SHA-1 digesting. No specific function for generating TPM_AuthData is specified by the TCG specification.
-msf <file_name>	Windows Vista-generated AuthData file if TPM owned.

2.2.2 BIOS and the LAN driver

The FW update guide that comes with the kits describes how to update BIOS and the LAN driver.

§

3 Intel® TPM impact on Intel® ME Firmware Update

3.1 Intel® TPM Specification Requirements

The TCG (Trusted Computing Group) specification strictly defines the method and procedure for updating TPM firmware (see the reference material section and TCG 1.2 Specification, Main Part 1, Section 15.1; and Main part 3, Section 9.1).

In the case of Intel® TPM, the firmware is integrated inside the Intel® ME and cannot be updated separately. This implies that all firmware needs to be updated whenever there's an update to the Intel® ME or the Intel® TPM.

3.2 Intel® TPM Firmware Update

As it is not possible to initiate the firmware update through the Intel® ME interface, the Intel® TPM interface must be used by all platforms that are considered Intel® TPM SKU.

An Intel® TPM SKU is defined as one where both of the following are true:

- Intel® TPM firmware is part of the Flash and is running.
- The Intel® TPM host interface is enabled via the soft-strap, hard-strap, and fuses (see section 3.4 for details).

FWUpdate first uses an Intel® ME interface message to determine whether or not the platform is an Intel® TPM SKU. The type of SKU in place determines which of the following flows is taken:

- If the image is an Intel® TPM SKU:
  1. FWUpdate sends all the partition packages via the Intel® TPM interface. This is done with the TPM_FieldUpgrade command.
  2. FWUpdate waits for an acknowledgement of the update.
  3. Once the update is completed, FWUpdate informs the user that the firmware has been updated:
  4. FWUpdate informs the user that the Intel® TPM is inoperable until a host reset occurs. (A reset is required after each successful firmware update.)
  5. FWUpdate reboots the OS.
- If the image is not an Intel® TPM SKU, the Intel® AMT-authorized FW update described in Table 2 is always allowed, though only via the TPM interface.
- If TPM is fused/strapped on, Intel® ME Firmware Update is only allowed via the TPM's interface and using the TPM's restrictions:
  - If TPM is unowned (a TPM operational state) – a physical presence must be provided in the form of a pop up question in the BIOS that you must approve/decline.

- If TPM is owned (a TPM owner has created a shared secret between the owner and the TPM) – owner authorization must be provided in the form of a passphrase or by delegation mechanism. (**Note**: This is not the same as Intel® AMT authorization, which has a different set of users, passwords, and permissions to perform actions.)

Table 2: AMT-authorized FW update

OEM	User Setting		
Override Counter	**Override Qualifer**	**MEBx setting**	**Anonymous ME FW Update**
0	N/a	Enabled Disabled	Enabled Disabled
0<n<255	N/a	N/a	Enabled for "n" host reboot cycles.
255	Never	Enabled Disabled	Enabled Disabled
255	Always	N/a	Enabled
255	Restricted	Enabled Disabled	Enabled until ME is provisioned Disabled

3.3 Impact of TPM State on Firmware Update

Firmware update authorization requirements differ with regard to the ownership state of the TPM. When TPM is owned, owner authorization is required to perform the firmware update. When TPM is not owned, a deferred assertion of physical presence is required for firmware update.

Below are the possible states and requirements for performing the firmware update:

- TPM owned: Owner-shared secret with TPM
- TPM unowned:
  - Deferred assertion of physical presence
  - Ownership taken temporarily.

Specification 1.2, Part 3, Section 9.1 states:

> TPM_FieldUpgrade is gated by either owner authorization or deferred assertion of Physical Presence (via the TPM_STCLEAR_DATA -> deferredPhysicalPresence -> unownedFieldUpgrade flag). This gating is acknowledgement that the entity that sets the security policy for a platform must approve field upgrade for that platform. This gating can block a global attack on TPMs when the TPME's privilege information (private key) has been compromised. For blocking to be effective in an unowned TPM, the TPM's ownership flag must be FALSE. (This prevents software from taking ownership and executing TPM_FieldUpgrade with owner authorization.)

If an owner is present, field upgrade MUST be owner authorized, as the actions indicate. This prevents an attacker from using physical presence to upgrade a TPM without detection by the owner.

The advantages of deferred assertion of Physical Presence are that it:

- permits a TPM to be upgraded if taking ownership is undesirable or impractical.
- permits a TPM to be upgraded in the OS environment (where Physical Presence typically cannot be asserted), when the TPM has no owner.

If it is acceptable to take ownership of a TPM temporarily, an alternative to deferred assertion of Physical Presence is the process: (1) take ownership; (2) perform an owner authorized field upgrade; (3) clear the owner from the TPM.

There is no requirement for patch confidentiality. Confidentiality may be implemented using a manufacturer specific mechanism, and may use a global secret such as a symmetric encryption key.

3.4 Straps and Fuses

Fuses are required on both ICH and MCH because Intel® TPM has HW functionality that is spread across ICH and MCH to help define the chipset SKUs. Straps are provided so that the OEM has the ability to enable/disable functionality at its end.

Table 3: Fuse and Strap Description

Name	Detailed Description
MCH Fuse	A fuse will be present in the MCH. If Blown (off), the fuse will disable Intel® TPM on the platform.
ICH Fuse	A fuse will be present in the ICH. If Blown (off), the fuse will disable Intel® TPM on the platform.
MCH Strap	A boot strap pin will be present on the MCH. OEM can implement it to activate Intel® TPM.
ICH Strap	A boot strap pin will be present on the ICH. OEM can implement it to activate Intel® TPM.
Soft Strap	The platform will employ a soft strap to disable Intel® TPM functionality, even if the motherboard hard straps are set to the "enabled" state. This soft strap will be stored in SPI Flash Descriptor region.

Fuses will override the straps. For Intel® TPM to be functional on the platform, all the fuses should be intact (ON) and all the pin straps should be sampled active (i.e., feature enabled). The correct settings for the fuses and pin straps are described in Table 4. The Flash soft strap will only be considered if the PCB resistor straps are in place and the silicon fuses are intact.

Table 4: Fuse and Strap Configuration

MCH Fuse	MCH PCB Strap Location	ICH Fuse	ICH PCB Strap Location	Flash Soft Strap Setting	Intel® TPM Functionality
Intact	Populated	Intact	Populated	Enabled	Enabled
Intact	Populate	Intact	Populated	Disabled	OEM Disabled
Intact	Empty	Intact	X	X	OEM Disabled
Intact	X	Intact	Empty	X	OEM Disabled
Blown	X	X	X	X	Intel Disabled
X	X	Blown	X	X	Intel Disabled

Note: In Table 4:
Intact = Enabled
Blown = Disabled
X = Doesn't matter

§

4 Generic update procedure for End User

4.1 Downloading and Extracting Upgrades

A BIOS update package must be obtained from the computer manufacturer who will most likely provide a combined BIOS and Intel® ME update package. This update package will typically be distributed as an EXE file. The following points must be checked:

- BIOS update package content - if it updates both BIOS and Intel® ME firmware, when platform has Intel® TPM there are the following restrictions on updating Intel® ME:
  - If the TPM is owned – a TPM Owner passphrase is required to authorize an Intel® ME Firmware update
  - If the TPM is not owned – the policy to authorize a Intel® ME Firmware update is executed by ME/MEBx and deferred physical presence, per TCG specification (by the BIOS).
- BIOS update package format - if it is an archive (use WinZip* or WinRAR* to verify):
  1. Extract the contents of the archive to a temporary directory.
  2. Copy the files needed for the BIOS upgrade to the working folder (i.e., *C:\AMT41\BIOS*).
  3. Note the name of the BIOS update utility (i.e., *UPDBIOS.exe*).
- BIOS update command line options - the BIOS update must run silently, without requiring any user prompts, and must be executable via the command line. A common way of finding which command line options are available is to run the update utility from the command line using the "***/?***" help switch (i.e., *C:\AMT41\BIOS\UPDBIOS.EXE /?*).

4.2 Performing the Upgrade

Follow your computer manufacturer's procedure and instructions for upgrading BIOS and/or Intel® ME firmware.

§

5 Appendix A: Bill of Materials (BOM)

- Manufacturing tool binaries
- Validation tool binaries for manufacturing floor validation
- Intel® ME FW image
- User desktop TPM icon SW binary
- Document supporting compliance claims
- Compliance tools binaries for Intel® TPM compliance testing

§