Intel® 7 Series Chipset - Intel® Management Engine 8.1 SKU

1.5 MB Firmware Getting Started User Guide

March 2012

Revision 1.0

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.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained at http://www.intel.com/design/literature.htm.

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

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.

Contents

Figures

Tables

Revision History

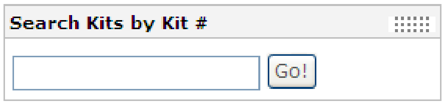
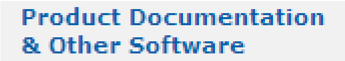
Document Number	Revision Number	Description	Revision Date
480305	0.5	Initial release of the document.	July 2011
480305	0.8	Updated product references and graphics	September 2011
480305	0.9	Updated and added HM70 to SKU Matrix	November 2011
480305	1.0	Updated SKU Matrix tables	March 2012

§ §

1 To-Do Checklist

The following checklist is intended to help you get started on using the Intel® Management Engine 1.5 MB Firmware (Intel® ME 1.5 MB FW) release kit.

Table 1. To-Do Checklist

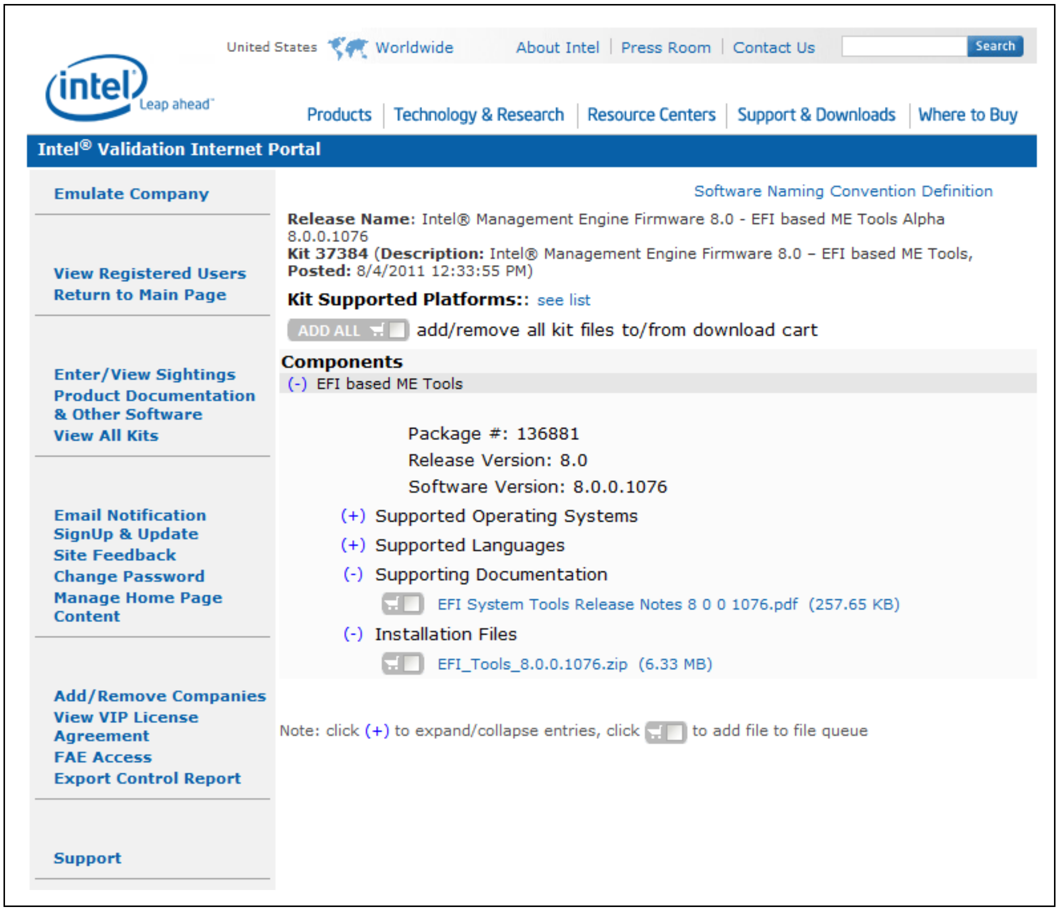
	What You Need To Do	How To Get It Done
□	Download the latest Intel® ME 1.5 MB FW kit from the Intel® Validation Internet Portal (VIP) website	Login to the *VIP* website at: https://platformsw.intel.com If you know the Kit #, use the box:  Search Kits by Kit # Otherwise, search for kit by Platform/Product. **Note:** Engineering releases will be stored under:  Product Documentation & Other Software This link is located on the left side of the *VIP Main Page*. Click on this link and search for "ME Firmware 8" to find latest Engineering release kit.
□	Create a Flash Image for your platform and Program Image onto the SPI Flash devices	Follow the *1.5 MB FW Bring Up Guide*, which is included with the kit. This document provides step-by-step instructions to create the Flash image. Details are also provided on how to program the image onto Serial Peripheral Interface (SPI) Flash devices and how to perform a quick check on firmware status.
□	Review the 1.5 MB FW Release Notes[1]	The *1.5 MB FW Release Notes*[1] document is included with the kit (see Figure 1 for location). This document provides Important Notes as well as Open and Closed Issues for this release. Review these sections for any special instructions required for this release. In addition, these sections identify areas to avoid and workarounds for your platform compliancy and validation testing.
□	Platform Validation and Compliancy	Login to VIP (https://platformsw.intel.com) and download Intel® ME Compliance and Debug Kit. This kit includes documents, tools and install packages for: • Intel® ME Test Suite (see 1.5 MB Compliance Guide) • Intel® Automated Power Switch • Intel® ME Debug Tool Follow documents for each component to test platform compliancy.

	What You Need To Do	How To Get It Done
□	Review Manufacturing Recommendations and Guidelines	The following documents will be available around **Beta** release timeframe: • Manufacturing Recommendations for Panther Point Platforms (available on Intel® Business Portal (IBP) https://businessportal.intel.com) • Manufacturing Advantage Service (MAS) for Panther Point Platforms (available on Intel® Learning Network (ILN) https://learn.intel.com) In addition, the System Tools User Guide (included with the kit) provides useful information on how to use the following tools in the manufacturing environment: Flash Programming Tool, FWUpdate, MEInfo and MEManuf.

[1] The *1.5 MB FW Release Notes* are included with the release kits on VIP but this document is not in the ".zip" Installation File. The Release Notes can be found in the "Supporting Documentation" section as shown below.

Contact your local Intel® representative if you have any questions.

Figure 1. VIP - Release Notes in Supporting Documentation



Release Name: Intel® Management Engine Firmware 8.0 - EFI based ME Tools Alpha 8.0.0.1076
Kit 37384 (**Description:** Intel® Management Engine Firmware 8.0 – EFI based ME Tools,
Posted: 8/4/2011 12:33:55 PM)

Kit Supported Platforms:: see list

ADD ALL add/remove all kit files to/from download cart

Components

(-) EFI based ME Tools

Package #: 136881
Release Version: 8.0
Software Version: 8.0.0.1076

(+) Supported Operating Systems
(+) Supported Languages
(-) Supporting Documentation
EFI System Tools Release Notes 8 0 0 1076.pdf (257.65 KB)
(-) Installation Files
EFI_Tools_8.0.0.1076.zip (6.33 MB)

Note: click (+) to expand/collapse entries, click to add file to file queue

§ §

2 Introduction

This document provides a guide to using the Intel® Management Engine 1.5 MB Firmware (Intel® ME 1.5 MB FW). Important overview details on the platform architecture bring up, compliancy and validation, and manufacturing topics are covered, along with details on where you can find additional information.

The Intel® ME 1.5 MB FW is stored on SPI Flash and executes on the Intel® 7 Series Chipset Family PCH. It enables unique, value-add consumer capability on Intel® 7 Series Chipset Family based platforms. These features are highlighted in the table below:

Table 2. Intel® ME 1.5 MB FW Features and Product SKUs

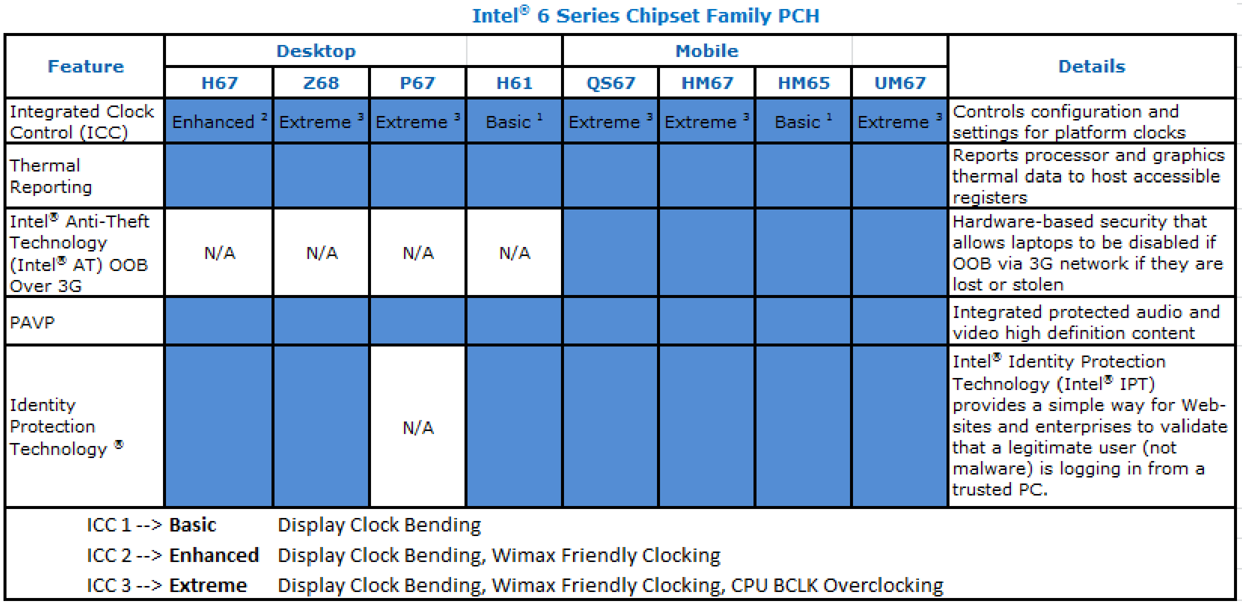
Intel® 7 Series Chipset Family PCH

Feature	Desktop			Mobile					Details
	H77	Z77	Z75	QS77	HM75	HM76	HM77	UM77	
Integrated Clock Control (ICC)	Enhanced [2]	Extreme [3]	Extreme [3]	Extreme [3]	Basic [1]	Basic [1]	Extreme [3]	Extreme [3]	Controls configuration and settings for platform clocks
Thermal Reporting	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	Reports processor and graphics thermal data to host accessible registers
Intel® Anti-Theft Technology (Intel® AT) OOB Over 3G	N/A	N/A	N/A	🟦	🟦	🟦	🟦	🟦	Hardware-based security that allows laptops to be disabled if OOB via 3G network if they are lost or stolen
PAVP	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	Integrated protected audio and video high definition content
Identity Protection Technology ®	N/A	N/A	N/A	🟦	🟦	🟦	🟦	🟦	Intel® Identity Protection Technology (Intel® IPT) provides a simple way for Web-sites and enterprises to validate that a legitimate user (not malware) is logging in from a trusted PC.

ICC 1 --> **Basic** Display Clock Bending

ICC 2 --> **Enhanced** Display Clock Bending, Wimax Friendly Clocking

ICC 3 --> **Extreme** Display Clock Bending, Wimax Friendly Clocking, CPU BCLK Overclocking



Intel® 6 Series Chipset Family PCH

Feature	Desktop				Mobile				Details
	H67	Z68	P67	H61	QS67	HM67	HM65	UM67	
Integrated Clock Control (ICC)	Enhanced [2]	Extreme [3]	Extreme [3]	Basic [1]	Extreme [3]	Extreme [3]	Basic [1]	Extreme [3]	Controls configuration and settings for platform clocks
Thermal Reporting	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	Reports processor and graphics thermal data to host accessible registers
Intel® Anti-Theft Technology (Intel® AT) OOB Over 3G	N/A	N/A	N/A	N/A	🟦	🟦	🟦	🟦	Hardware-based security that allows laptops to be disabled if OOB via 3G network if they are lost or stolen
PAVP	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	Integrated protected audio and video high definition content
Identity Protection Technology ®	🟦	🟦	N/A	🟦	🟦	🟦	🟦	🟦	Intel® Identity Protection Technology (Intel® IPT) provides a simple way for Web-sites and enterprises to validate that a legitimate user (not malware) is logging in from a trusted PC.

ICC 1 --> **Basic** Display Clock Bending

ICC 2 --> **Enhanced** Display Clock Bending, Wimax Friendly Clocking

ICC 3 --> **Extreme** Display Clock Bending, Wimax Friendly Clocking, CPU BCLK Overclocking

For more information regarding the firmware features listed above, please refer to the appropriate Product Requirements Document (PRD), which can be downloaded from the Intel® Business Portal (IBP) website at https://businessportal.intel.com.

For platform enabling details about Intel® AT Technology, contact your local Intel sales representative, or refer to: http://www.intel.com/technology/anti-theft/ for general information.

§ §

3 Platform Architecture Overview

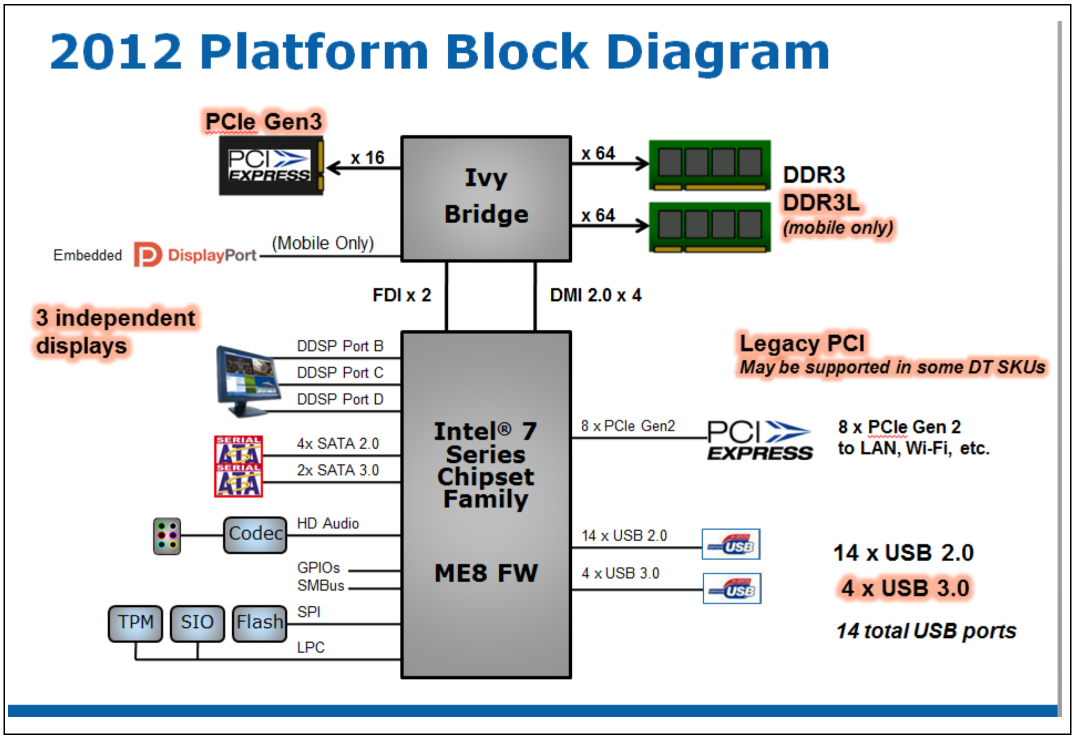
Platform requirements needed to properly support the Intel® ME 1.5 MB FW include:

- Ivy Bridge-based Core family processor
- Intel® 7 Series Chipset Platform Controller Hub (PCH)
- Hardware design based on Intel® Customer Reference Board (CRB) - Maho Bay Desktop CRB or Chief River Mobile CRB

The following hardware documents and design files are available on IBP (https://businessportal.intel.com):

- Maho Bay and Chief River Platform Design Guides
- Maho Bay and Chief River Schematics, Layout files and IBIS Models
- Ivy Bridge Processor External Design Specification
- Panther Point PCH External Design Specification

Figure 2. Platform Architecture and Components



§ §