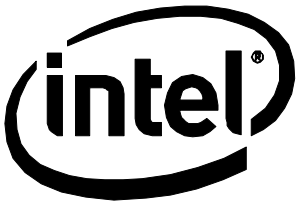

+

Intel® Compute Card
CD1M3128MK
CD1IV128MK
Technical Product Specification

August 2017
Order Number: J46734-001

Intel® Compute Card CD1M3128MK or CD1IV128MK may contain design defects or errors known as errata that may cause the product to deviate from published specifications. Current characterized errata, if any, are documented in Intel® Compute Card CD1M3128MK or CDIV128MK Specification Updates

Revision History

Revision	Revision History	Date
001	First release	August 2017

Disclaimer

This product specification applies to only the standard Intel® Compute Card with BIOS identifier MKKBLY35.86A or MKKBI5V.86A.

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.

All Compute Cards are evaluated as Information Technology Equipment (I.T.E.) for installation in homes, offices, schools, computer rooms, and similar locations. The suitability of this product for other PC or embedded non-PC applications or other environments, such as medical, industrial, alarm systems, test equipment, etc. may not be supported without further evaluation by Intel.

Intel Corporation may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights that relate to the presented subject matter. The furnishing of documents and other materials and information does not provide any license, express or implied, by estoppel or otherwise, to any such patents, trademarks, copyrights, or other intellectual property rights.

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.

Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families: Go to:
Learn About Intel® Processor Numbers

Contact your local Intel sales office or your distributor to obtain the latest specifications before placing your product order.

Intel, the Intel logo and Intel Core are trademarks of Intel Corporation in the U.S. and/or other countries.

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

Specification Changes or Clarifications

The table below indicates the Specification Changes or Specification Clarifications that apply to the Intel® Compute Card CD1M3128MK and CD1IV128MK.

Specification Changes or Clarifications

Date	Type of Change	Description of Changes or Clarifications
		•

Errata

Current characterized errata, if any, are documented in a separate Specification Update. See http://www.intel.com/ComputeCardSupport for the latest documentation.

Preface

This Technical Product Specification (TPS) specifies the layout, components, connectors, power, environmental and BIOS features for the Intel® Compute Card CD1M3128MK and CD1IV128MK.

NOTE

In this document, the use of “Intel® Compute Card” will refer to the CD1M3128MK and CD1IV128MK versions of the Intel® Compute Card.

Intended Audience

The TPS is intended to provide detailed technical information about Intel® Compute Card CD1M3128MK and CD1IV128MK and its components to the vendors, system integrators, and other engineers and technicians who need this level of information. It is specifically not intended for general audiences.

What This Document Contains

Chapter	Description
1	A description of the hardware used on Intel® Compute Card CD1M3128MK and CD1IV128MK
2	A technical description of the Intel® Compute Card CD1M3128MK and CD1IV128MK
3	The features supported by the BIOS Setup program

Typographical Conventions

This section contains information about the conventions used in this specification. Not all of these symbols and abbreviations appear in all specifications of this type.

Notes, Cautions, and Warnings

NOTE

Notes call attention to important information.

CAUTION

Cautions are included to help you avoid damaging hardware or losing data.

Other Common Notation

#	Used after a signal name to identify an active-low signal (such as USBP0#)
GB	Gigabyte (1,073,741,824 bytes)
GB/s	Gigabytes per second
Gb/s	Gigabits per second
KB	Kilobyte (1024 bytes)
Kb	Kilobit (1024 bits)
kb/s	1000 bits per second
MB	Megabyte (1,048,576 bytes)
MB/s	Megabytes per second
Mb	Megabit (1,048,576 bits)
Mb/s	Megabits per second
TDP	Thermal Design Power
Xxh	An address or data value ending with a lowercase h indicates a hexadecimal value.
x.x V	Volts. Voltages are DC unless otherwise specified.
*	This symbol is used to indicate third-party brands and names that are the property of their respective owners.

Contents

Figures

Tables

1 Product Description

1.1 Overview

The Intel® Compute Card requires a certified compatible device with a Compute Card slot in order to operate. For information on compatible devices for use with the Intel® Compute Card see www.intel.com/ComputeCard/.

1.2 Version Summary

There are two different versions of this model of Intel® Compute Card available which are summarized in Table 1. Unless otherwise noted in this document, not all features are available on all versions of the Intel® Compute Cards.

Table 1. Version Summary

Version	Intel® vPro™	Discrete TPM	Memory	Processor
CD1M3128MK	No	No	4 GB	Intel® Core™ m3-7Y30 Processor
CD1IV128MK	Yes	Yes	8 GB	Intel® Core™ i5-7Y57 Processor

1.3 Online Support

To find information about…	Visit this World Wide Web site:
Intel® Compute Card	http://www.intel.com/ComputeCard
Intel® Compute Card CD1M3128MK and CD1IV128MK Support	http://www.intel.com/ComputeCardSupport
Available configurations for Intel® Compute Card	http://ark.intel.com

1.4 Feature Summary

Table 2 summarizes the major features of the Intel® Compute Card.

Table 2. Feature Summary

Form Factor	94.5 millimeters by 55 millimeters by 5 millimeters (3.7205 inches by 2.1654 inches by 0.1969 inches)
Processor	• Soldered-down Intel® Core™ processor — Integrated graphics — Integrated memory controller — Integrated PCH
Memory	• Soldered-down dual-channel LPDDR3 1866 MHz memory • 4 GB total memory for CD1M3128MK • 8 GB total memory for CD1IV128MK
Graphics	Integrated graphics support with Intel® HD Graphics Technology
Audio	Intel® High Definition (Intel® HD) Audio
Storage	128 GB soldered-down PCIe x2 SSD onboard storage
BIOS	• Intel® BIOS resident in the Serial Peripheral Interface (SPI) Flash device • Support for Advanced Configuration and Power Interface (ACPI), Plug and Play, and System Management BIOS (SMBIOS)
Wireless LAN	Soldered-down Intel® Dual Band Wireless-AC module • 802.11a/b/g/n, 802.11ac, Bluetooth* 4.2 • Supports Miracast* and Miracast Plus
Advanced Technologies	• Intel® vPro™ Technology (CD1IV128MK only) • Intel® Virtualization Technology (VT-x) • Intel® Virtualization for Directed I/O (VT-d) • Intel® VT-x with Extended Page Tables (EPT) • Intel® Speed Shift Technology • Intel® Turbo Boost Technology • Intel® Hyper-Threading Technology • Enhanced Intel® SpeedStep® Technology • Intel® Identity Protection Technology (Intel® IPT) • Intel® Platform Trust Technology (Intel® PPT) – (CD1M3128MK only)
Security and Reliability	• Intel® Active Management Technology 11.0 (Intel® AMT) – (CD1IV128MK only) • Intel® Trusted Execution Technology (Intel® TXT) – (CD1IV128MK only) • Intel® Memory Protection Extensions (Intel® MPX) • Intel® Software Guard Extensions (Intel® SGX) • Intel® AES New Instructions • Execute Disable Bit • Discreet Trusted Platform Module 2.0 (TPM) – (CD1IV128MK only)

To find information about...	Visit this World Wide Web site:
Advanced Technologies Security and Reliability	http://www.intel.com/Support

1.4.1 Compute Card Exterior

Figures 1 and 2 show the exterior of the Intel® Compute Card.

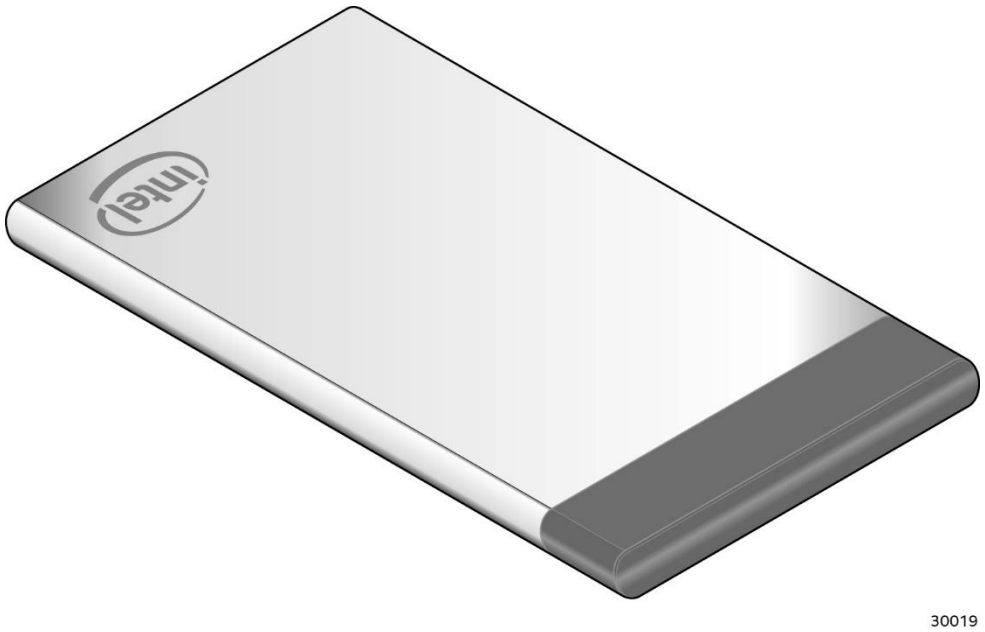

Figure 1. Top-Front View of Compute Card

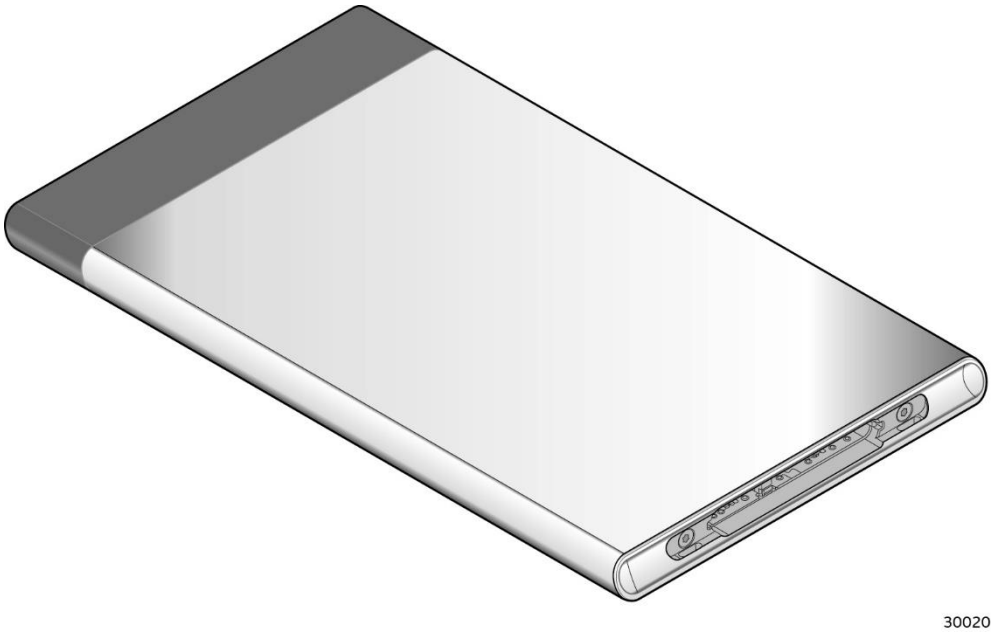

Figure 2. Bottom-Back View of Compute Card

1.4.2 Block Diagram

Figure 3 is a block diagram of the major functional areas of the Intel® Compute Card.

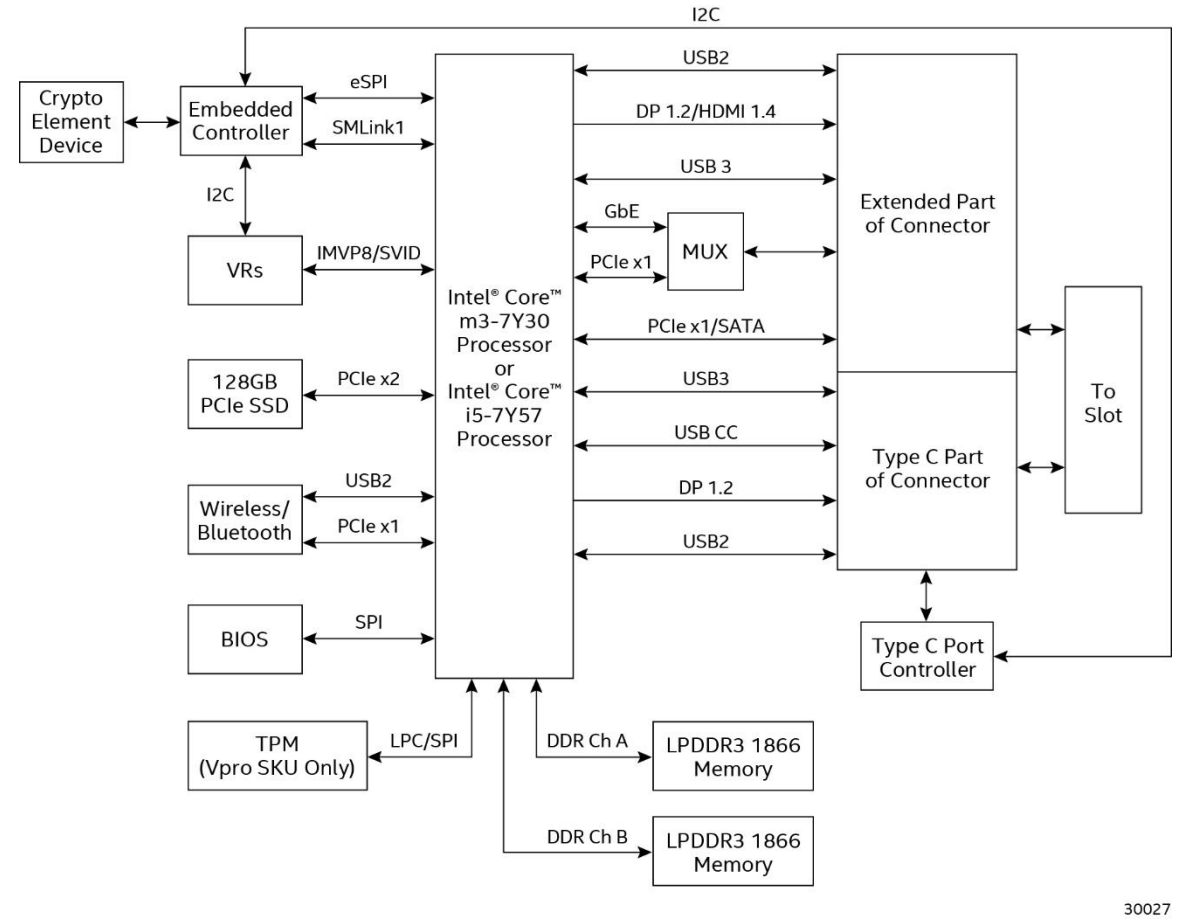

Figure 3. Block Diagram

1.5 Operating System Overview

The Intel® Compute Card CD1M3128MK and CD1IV128MK support the following Operating Systems (64-bit only).

- Windows* 10 Home
- Windows 10 Pro
- Windows 10 Enterprise
- Windows 10 Education
- Windows 10 IoT Enterprise
- Some Linux* operating systems may be supported. Check with the specific Linux distribution to make sure that support is available for this platform.

Installation of any of the above operating systems will require a compatible device with a Compute Card slot, the Compute Card plugged in, a mouse and keyboard along with a USB flash drive or USB optical drive. The USB flash drive or USB optical drive will need the operating system installation media.

To find information about…	Visit this World Wide Web site:
Intel® Compute Card drivers	http://downloadcenter.intel.com

1.6 Processor

The Intel® Compute Card has a soldered-down System-on-a-Chip (SoC), which consists of an Intel® Core™ m3-7Y30 Processor on the CD1M3128MK and an Intel® Core™ i5-7Y57 Processor on the CD1IV128MK.

- Integrated Intel® HD Graphics 615
- Integrated memory controller
- Integrated PCH

1.7 System Memory

The Intel® Compute Card has soldered-down memory and supports the following memory features:

- LPDDR3 1866 MHz
- Dual-channel memory
- 2 GB memory per channel (4 GB total memory) on CD1MK128MK
- 4 GB memory per channel (8 GB total memory) on CD1IV128MK
- Refer to Section 2.1 on page 24 for information on the total amount of addressable memory

1.8 System Storage

The Intel® Compute Card has soldered-down storage using a 128 GB PCIe x2 Sold State Drive.

1.9 Processor Graphics Subsystem

The Intel® Compute Card supports graphics through Intel® HD Graphics.

1.9.1 Integrated Graphics

The Intel® Compute Card supports integrated graphics via the processor. Two Digital Display Interface (DDI) lanes are available from the Compute Card connector. How the DDI lanes are used is dependent on the device the Compute Card is plugged into and how the lanes are configured. By default, the DDI lanes are configured as DisplayPort* 1.2. The DDI lane from the extended part of the connector can be configured as HDMI* 1.4b via DDI_Config.

- High-Bandwidth Digital Content Protection support for content protection
  - HDCP 2.2 supported via DisplayPort
  - HDCP 1.4 supported via HDMI
- Resolutions and refresh rates supported
  - Up to 4K @ 60Hz via DisplayPort
  - Up to 4K @ 30Hz via HDMI

See section 2.2 for more information on the connector and connector configuration options.

1.9.1.1 Intel® High Definition (Intel® HD) Graphics

The Intel® HD graphics controller features the following:

- 3D graphics hardware acceleration supporting Direct3D* 9/1011.1/11.2, DirectX*11, Direct2D, OpenCL 2.0/2.1, OpenGL 5.0
- Video decode hardware acceleration supporting AVC/H264, HEVC/H265, JPEG, MJPEG, MPEG2, VC1/WMV9, VP8 and VP9 formats
- Video encode hardware acceleration supporting AVC/H264, HEVC/H265, JPEG, MJPEG, MPEG2, VC-1, VP8 and VP9

1.9.1.2 Video Memory Allocation

Intel® Dynamic Video Memory Technology (DVMT) is a method for dynamically allocating system memory for use as graphics memory to balance 2D/3D graphics and system performance. If your computer is configured to use DVMT, graphics memory is allocated based on system requirements and application demands (up to the configured maximum amount). When memory is no longer needed by an application, the dynamically allocated portion of memory is returned to the operating system for other uses.

1.9.1.3 Integrated Audio

The following audio technologies are supported via the Digital Display Lanes using either DisplayPort or HDMI:

- AC3 Dolby* Digital
- Dolby Digital Plus
- DTS-HD*
- LPCM, 192 kHz/16-bit or 176.4kHz/24-bit, 8 Channel
- Dolby TrueHD, DTS-HD Master Audio*

1.10 Wireless LAN Subsystem

The Intel® Compute Card wireless LAN subsystem consists of the following:

- Intel® Dual Band Wireless-AC 8265 module
- 1216 BGA soldered-down

For information about	Refer to
LAN software and drivers	http://downloadcenter.intel.com

1.10.1 Wireless Network Module

The Dual Band Wireless-AC 8265 module provides hi-speed wireless connectivity with the following capabilities:

- 802.11a/b/g/n, 802.11ac
- 2.4 GHz, 5.0 GHz
- Two antennas incorporated inside the Compute Card
- Dual Mode Bluetooth 4.2
- Supports Miracast* and Miracast Plus
- Support for AMT 11.0 on CD1IV128MK

For information about	Refer to
Obtaining WLAN software and drivers	http://downloadcenter.intel.com
Full Specifications	http://intel.com/wireless

1.11 Authentication

The Intel® Compute Card and any device with a compatible slot for the Intel® Compute Card will use bidirectional authentication. The Compute Card will attempt to authenticate the compatible device and the compatible device will attempt to authenticate the Compute Card. The authentication uses digital keys, which are provisioned by default during manufacturing for every Compute Card and Compute Card compatible device. With this provisioning, the Intel® Compute Card will only work with correctly provisioned Intel® Compute Card slot compatible devices.

1.12 Power Management

Power management is implemented at several levels, including:

- Software support through Advanced Configuration and Power Interface (ACPI)
- Hardware support:
  - Power Input
  - Instantly Available PC technology
  - Wireless LAN wake capabilities
  - Wake from USB (When plugged into a compatible device)
  - Wake from S5

1.12.1 ACPI

ACPI gives the operating system direct control over the power management and Plug and Play functions of a computer. The use of ACPI with this Compute Card requires an operating system that provides full ACPI support. ACPI features include:

- Plug and Play (including bus and device enumeration)
- Power management control of individual devices
- A Soft-off feature that enables the operating system to power-off the Compute Card
- Support for multiple wake-up events (see Table 5 on page 19)

Table 3 lists the system states based on how long the power switch is pressed, depending on how ACPI is configured with an ACPI-aware operating system. Support is only available when the Compute Card is plugged into a compatible device's Compute Card slot.

Table 3. Effects of Pressing the Power Switch

If the system is in this state...	...and the power switch is pressed for	...the system enters this state
Off (ACPI G2/G5 – Soft off)	Less than four seconds	Power-on (ACPI G0 – working state)
On (ACPI G0 – working state)	Less than four seconds	Soft-off/Standby (ACPI G1 – sleeping state) Note
On (ACPI G0 – working state)	More than six seconds	Fail safe power-off (ACPI G2/G5 – Soft off)
Sleep (ACPI G1 – sleeping state)	Less than four seconds	Wake-up (ACPI G0 – working state)
Sleep (ACPI G1 – sleeping state)	More than six seconds	Power-off (ACPI G2/G5 – Soft off)

Note: Depending on power management settings in the operating system.

1.12.1.1 System States and Power States

Under ACPI, the operating system directs all system and device power state transitions. The operating system puts devices in and out of low-power states based on user preferences and knowledge of how devices are being used by applications. Devices that are not being used can be turned off. The operating system uses information from applications and user settings to put the system as a whole into a low-power state.

Table 4 lists the power states supported by the Compute Card along with the associated system power targets. See the ACPI specification for a complete description of the various system and power states.

Table 4. Power States and Targeted System Power

Global States	Sleeping States	Processor States	Device States	Targeted System Power (Note 1)
G0 – working state	S0 – working	C0 – working	D0 – working state.	Full power
G1 – sleeping state	S3 – Suspend to RAM. Context saved to RAM.	No power	D3 – no power except for wake-up logic.	Power < 5 W (Note 2)
G1 – sleeping state	S4 – Suspend to disk. Context saved to disk.	No power	D3 – no power except for wake-up logic.	Power < 5 W (Note 2)
G2/S5	S5 – Soft off. Context not saved. Cold boot is required.	No power	D3 – no power except for wake-up logic.	Power < 5 W (Note 2)
G3 – mechanical off AC power is disconnected	No power to the system.	No power	D3 – no power for wake-up logic.	No power to the system. Service can be performed safely.

Notes:

1. Total system power is dependent on the system configuration and peripherals powered by the system power supply.
2. Dependent on the standby power consumption of wake-up devices used in the system.

1.12.1.2 Wake-up Devices and Events

Table 5 lists the devices or specific events that can wake the Compute Card from specific states.

Table 5. Wake-up Devices and Events

Devices/events that wake up the system…	…from this sleep state	Comments
Power switch	S3, S4, S5	Only supported if compatible device has a power switch
RTC alarm	S3, S4, S5 (Note 1, 3)	
Wireless LAN	S3, S4, S5 (Notes 1, 2, 3, 4)	"S5 WOL after G3" supported
USB	S3, S4 (Note 3, 4)	Wake S4 controlled by BIOS option. Only supported if compatible device has USB ports.
Bluetooth	S3	
PCIe controller on slot	S3, S4, S5 (Notes 1, 2)	Only supported if compatible device has support for wake events

Notes:

1. Monitor will remain in "sleep" state from S3 resume.
2. "S5 WoL after G3" only supported w/Deep Sleep disabled
3. Wake from S4 only supported w/Deep Sleep disabled
4. Wake from device/event not supported immediately upon return from AC loss
5. Wake from S5 only supported on CD1IV128MK

NOTE

The use of these wake-up events from an ACPI state requires an operating system that provides full ACPI support. In addition, software, drivers, and peripherals must fully support ACPI wake events.

1.12.2 Hardware Support

Power management hardware features include the following when the Compute Card is plugged into a compatible device's slot:

- Wake from Power Button signal
- Instantly Available PC technology
- Wireless LAN wake capabilities
- Wired LAN wake capabilities
- Wake from USB
- Wake from S5

NOTE

The use of Wake from USB from an ACPI state requires an operating system that provides full ACPI support.

1.12.2.1 Instantly Available PC Technology

Instantly Available PC technology enables the Compute Card to enter the ACPI S3 (Suspend-to-RAM) sleep-state. While in the S3 sleep-state, the computer will appear to be off (the power supply is off, and the front panel off). When signaled by a wake-up device or event, the system quickly returns to its last known wake state. Table 5 on page 19 lists the devices and events that can wake the Compute Card from the S3 state when the Compute Card is plugged into a compatible device.

The use of Instantly Available PC technology requires operating system support.

1.12.2.2 Wired LAN Wake Capabilities

Wired LAN wake capabilities enable remote wake-up of the Compute Card through a network. The Wired LAN subsystem monitors network traffic at the Media Independent Interface. Upon detecting a Magic Packet* frame, the Wired LAN subsystem asserts a wake-up signal that powers up the Compute Card. Only available when plugged into a compatible device that has support for Wired LAN.

1.12.2.3 Wireless LAN Wake Capabilities

Wireless LAN wake capabilities enable remote wake-up of the Compute Card through a network. The Wireless LAN subsystem monitors network traffic at the Media Independent Interface. Upon detecting a Magic Packet* frame, the Wireless LAN subsystem asserts a wake-up signal that powers up the Compute Card.

1.12.2.4 Wake from USB

USB activity wakes the Compute Card from an ACPI S3 and S4 states.

NOTE

Wake from USB requires the use of a USB peripheral that is plugged into a compatible device that supports Wake from USB.

1.12.2.5 Wake from S5

When the RTC Date and Time is set in the BIOS, the Compute Card will automatically wake from an ACPI S5 state.

1.13 Intel® Security and Manageability Technologies

Intel® Security and Manageability Technologies provides tools and resources to help small business owners and IT organizations protect and manage their assets in a business or institutional environment.

NOTE

Software with security and/or manageability capability is required to take advantage of Intel platform security and/or management technologies.

1.13.1 Intel® vPro™ Technology

Only available on the CD1IV128MK. Intel® vPro™ Technology is a collection of platform capabilities that support enhanced manageability, security, virtualization and power efficiency. The key platform capabilities include:

- Intel® Active Management Technology (Intel® AMT) 11.0
- Intel® Virtualization (Intel® VT)
- Intel® Virtualization for Directed I/O (Intel® VT-d)
- Intel® Trusted Execution Technology (Intel® TXT)
- Intel® Identity Protection Technology (Intel® IPT)
- Trusted Platform Module 2.0 (TPM)

For information about	Refer to
Intel® vPro Technology	http://www.intel.com/content/www/us/en/support/technologies/intel-vpro-technology.html

1.13.1.1 Intel® Active Management Technology 11.0

Only available on the CD1IV128MK. When used with third-party management and security applications, Intel® Active Management Technology (Intel® AMT) allows business owners and IT organizations to better discover, heal, and protect their networked computing assets.

Some of the features of Intel® AMT include:

- Out-of-band (OOB) system access, to discover assets even while PCs are powered off
- Remote trouble-shooting and recovery, which allows remote diagnosis and recovery of systems after OS failures
- Hardware-based agent presence checking that automatically detects and alerts when critical software agents have been stopped or are missing
- Proactive network defense, which uses filters to block incoming threats while isolating infected clients before they impact the network
- Remote hardware and software asset tracking, helping to track computer assets and keep virus protection up-to-date
- Keyboard, video and mouse (KVM) remote control, which allows redirection of a managed system's video to a remote console which can then interact with it using the console's own mouse and keyboard

NOTE

Intel® AMT requires the Compute Card to have network hardware and software, as well as connection with a power source, a corporate network connection, and an Intel® AMT-enabled remote management console. Setup requires additional configuration of the platform.

For information about	Refer to
Intel® Active Management Technology	http://www.intel.com/technology/platform-technology/intel-amt/index.htm

1.13.2 Intel® Virtualization Technology

Intel® Virtualization Technology (VT-x) is a hardware-assisted technology that, when combined with software-based virtualization solutions, provides maximum system utilization by consolidating multiple environments into a single server or client.

NOTE

A processor with Intel VT does not guarantee that virtualization will work on your Compute Card. Intel VT requires enabling software and/or operating system, device drivers, and applications designed for this feature.

For information about	Refer to
Intel® Virtualization Technology	http://www.intel.com/technology/virtualization/technology.htm

1.13.2.1 Intel® Virtualization Technology for Directed I/O

Intel® Virtualization Technology for Directed I/O (VT-d) allows addresses in incoming I/O device memory transactions to be remapped to different host addresses. This provides Virtual Machine Monitor (VMM) software with:

- Improved reliability and security through device isolation using hardware assisted remapping.
- Improved I/O performance and availability by direct assignment of devices.

1.13.2.2 Intel® VT-x with Extended Page Tables

Intel® VT-x with Extended Page Tables (EPT), also known as Second Level Address Translation (SLAT), provides acceleration for memory intensive virtualized applications. Extended Page Tables in Intel® Virtualization Technology platforms reduces the memory and power overhead costs and increases battery life through hardware optimization of page table management.

1.13.3 Intel® Trusted Execution Technology

Only available on the CD1IVMK128MK. Intel® Trusted Execution Technology (Intel® TXT) is a hardware security solution that protects systems against software-based attacks by validating the behavior of key components at startup against a known good source. It requires that Intel® VT be enabled and the presence of a TPM.

1.13.4 Intel® Identity Protection Technology

Intel® Identity Protection Technology (Intel® IPT) provides a simple way for websites and enterprises to validate that a user is logging in from a trusted computer. This is accomplished by using the Intel® Manageability Engine embedded in the chipset to generate a six-digit number that, when coupled with a user name and password, will generate a One-Time Password (OTP) when visiting Intel® IPT-enabled websites. Intel® IPT eliminates the need for the additional token or key fob required previously for two-factor authentication.

For information about	Refer to
Intel® Identity Protection Technology	http://ipt.intel.com

1.13.5 Intel® Platform Trust Technology (PTT)

Intel® PTT is a hardware firmware based TPM 2.0 implementation integrated in Intel® Management Engine (ME) for credential storage and key management. It provides a secure trust element to meet Microsoft Windows* 10 requirements for TPM 2.0 and Measured Boot for systems on which TPM 2.0 is required by Microsoft.

1.13.6 Intel® Software Guard Extensions (SGX)

Intel® Software Guard Extensions (Intel® SGX) provide applications the ability to create hardware enforced trusted execution protection for their applications' sensitive routines and data. Run-time execution is protected from observation or tampering by any other software (including privileged software) in a system.

1.13.7 Intel® Memory Protection Extensions (MPX)

Intel® Memory Protection Extensions (Intel® MPX) provides a set of hardware features that can be used by software in conjunction with compiler changes to check that memory references intended at compile time do not become unsafe at runtime due to buffer overflow or underflow.

1.13.8 Trusted Platform Module (discrete TPM)

Only available on the CD1IV128MK. The TPM version 2.0 component is specifically designed to enhance platform security above-and-beyond the capabilities of today's software by providing a protected space for key operations and other security critical tasks. Using both hardware and software, the TPM protects encryption and signature keys at their most vulnerable stages—operations when the keys are being used unencrypted in plain-text form. The TPM shields unencrypted keys and platform authentication information from software-based attacks.

NOTE

Support for TPM version 2.0 requires a UEFI-enabled operating system.

For information about	Refer to
Nuvoton NPCT650AAAYx	www.nuvoton.com

2 Technical Reference

2.1 Addressable Memory

The Intel® Compute Card utilizes up to 4 or 8 GB of addressable system memory depending on the model. Typically the address space that is allocated for PCI Conventional bus add-in cards, PCI Express configuration space, BIOS (SPI Flash device), and chipset overhead resides above the top of DRAM (total system memory). On a system that has 4 GB of system memory installed, it is not possible to use all of the installed memory due to system address space being allocated for other system critical functions. These functions include the following:

- 64 Mb BIOS/SPI Flash device for CD1M3128MK
- 128 Mb BIOS/SPI Flash device for CD1IV128MK
- Local APIC (19 MB)
- Direct Media Interface (40 MB)
- PCI Express configuration space (256 MB)
- SoC base address registers PCI Express ports (up to 256 MB)
- Integrated graphics shared memory (64 MB)

The Intel® Compute Card provides the capability to reclaim the physical memory overlapped by the memory mapped I/O logical address space. Physical memory is remapped from the top of usable DRAM boundary to the 4 GB boundary to an equivalent sized logical address range located just above the 4 GB boundary. All installed system memory can be used when there is no overlap of system addresses.

2.2 Connector

This section describes the connector available on the Intel® Compute Card. The connector is separated into two sections: a Type C-compliant portion and an extended portion. The Type C portion supports Type C-compliant connections including video with audio and USB. The extended portion supports video with audio, USB, and PCIe. Power is supplied to the card from the device the Compute Card is plugged into using the Type C portion of the connector.

2.2.1 Connector Interface Options

The connector has several interface options that are listed in table 6.

Table 6. Connector Interface Options

Interface	Type C Only Option A	Type C Only Option B	Type C + Extension Option A	Type C + Extension Option B
Digital Display Interface (DDI)	4 lanes	2 lanes	4 lanes over Type C 4 lanes over extension	2 lanes over Type C 4 lanes over extension
USB 3.0	0	1	1	2
USB 2.0	1	1	2	2
PCI Express or SATA	0	0	2	2
Power	Yes	Yes	Yes	Yes

- 2 lanes of DDI supports 1080P and 4 lanes of DDI supports 4K with DisplayPort 1.2
- Either DisplayPort or HDMI can be configured over DDI on the connector extension
- Only DisplayPort is supported over DDI on the Type C portion of the connector

2.2.2 Power On Straps and Select Signals

The connector has power on straps and select signals to define the interface. The options that can be selected are listed in table 7.

Table 7. Power On Straps and Select Signals

Pin	Description	Implementation
PE1_SEL*	PCE Express / SATA	VDM
PE2_SEL*	PCE Express / SATA	VDM
GbE_PE_SEL	LAN / PCI Express	Select VDM
PE_Wake#	PCIe Wake Event	VDM
CLK_REQ2#	PCIe Clock Request	Pin / Signal
CLK_REQ1#	PCIe Clock Request	Pin / Signal
DDI_Config**	DDI DP* / HDMI* Select	Pin / Signal
DDI_HPD	DDI Hot Plug Detect	Pin / Signal

*PE1_SEL and PE2_SEL support PCI Express / SATA selection

**DDI_Config supports DP++ (DP/HDMI select)

2.2.3 Muxing Options

Ethernet Controllers implementing a fully integrated media access controller (MAC) and physical layer interface (PHY) with a PCI Express connection may be connected to either PCI Express port.

Intel® Ethernet Connection physical layer (PHY) devices must be connected to HSIO2_TX/RX (pins D14/D15 and C14/C15). The device must send the appropriate VDM during power on negotiation to select Ethernet function. Intel® Ethernet Connection physical layer (PHY) devices may not be supported on all Compute Card compatible devices, please check the product specification for the Compute Card device intending to be supported.

HSIO1_RX/TX and HSIO2_RX/TX can be selected for either PCI Express or Serial ATA (SATA) operation. The device must send the appropriate VDM during power on negotiation to select the desired operating mode.

Display options for the connector extension can be selected for either HDMI or DisplayPort using DDI_Config.

2.2.4 Connector Pinout

The Intel® Compute Card has a single connector that supports the following signals shown in Table 8.

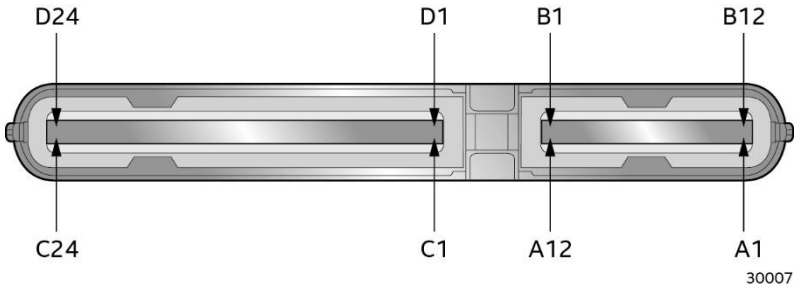

Figure 4. Compute Card Connector Pinout

Table 8. Compute Card Connector Pinout

Pin	Signal	Pin	Signal	Pin	Signal	Pin	Signal
D1	GND	C1	GND	B12	GND	A1	GND
D2	DDI2_L1-	C2	DDI2_L0-	B11	RX1+	A2	TX1+
D3	DDI2_L1+	C3	DDI2_L0+	B10	RX1-	A3	TX1-
D4	PE_RST#	C4	RSVD1	B9	Vbus	A4	Vbus
D5	DDI_Config	C5	DDI_HPD	B8	SBU2	A5	CC1
D6	DDI_L2-	C6	DDI_L3-	B7	USB1_D1-	A6	USB1_D1+
D7	DDI_L2+	C7	DDI_L3+	B6	USB1_D1+	A7	USB1_D1-
D8	CLK_REQ2#	C8	CLK_REQ1#	B5	CC2	A8	SBU1
D9	GND	C9	GND	B4	Vbus	A9	Vbus
D10	HSIO1_TX-	C10	HSIO1_RX-	B3	TX2-	A10	RX2-
D11	HSIO1_TX+	C11	HSIO1_RX+	B2	TX2+	A11	RX2+
D12	RefCLK1-	C12	RefCLK2-	B1	GND	A12	GND
D13	RefCLK1+	C13	RefCLK2+	NA	NA	NA	NA
D14	HSIO2_TX-	C14	HSIO2_RX-	NA	NA	NA	NA
D15	HSIO2_TX+	C15	HSIO2_RX+	NA	NA	NA	NA
D16	GND	C16	GND	NA	NA	NA	NA
D17	SMLINK_DATA	C17	SMLINK_CLK	NA	NA	NA	NA
D18	USB3_D-	C18	AUX2/Data2	NA	NA	NA	NA
D19	USB3_D+	C19	AUX2+/Clk2	NA	NA	NA	NA
D20	RSVD2	C20	GND	NA	NA	NA	NA
D21	RSVD3	C21	RSVD4	NA	NA	NA	NA
D22	SS_RX-	C22	SS_TX-	NA	NA	NA	NA
D23	SS_RX+	C23	SS_TX+	NA	NA	NA	NA
D24	GND	C24	GND	NA	NA	NA	NA

2.3 Power Considerations

The Compute Card requires a DC input via the Type C portion of the connector supplied over the connector via USB Power Delivery Protocol from the device that the Compute Card is plugged into:

- Voltage: 12 V +/-5%
- Current (RMS max): 1.67 A
- Current (Peak): 2.62 A

2.4 Mechanical Considerations

2.4.1 Form Factor

Figure 5, Figure 6, Figure 7 and Figure 8 illustrate the mechanical form factor for the Intel® Compute Card. Dimensions are given in millimeters.

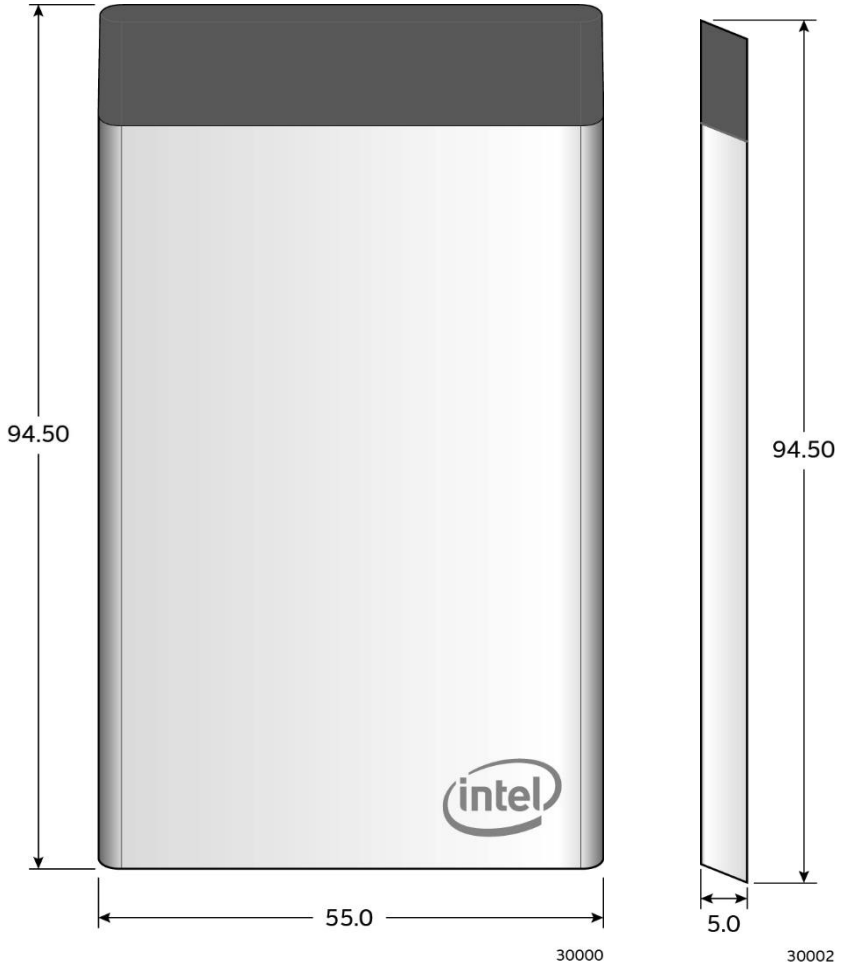

Figure 5. Compute Card Dimensions (Top and Left)

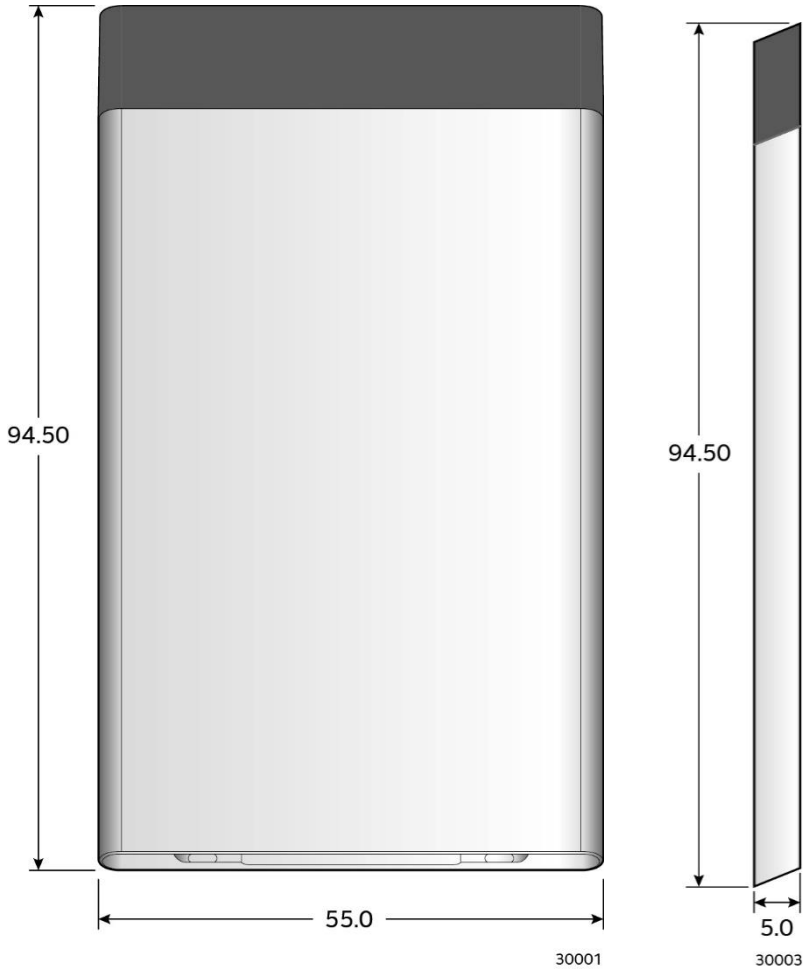

Figure 6. Compute Card Dimensions (Bottom and Right)

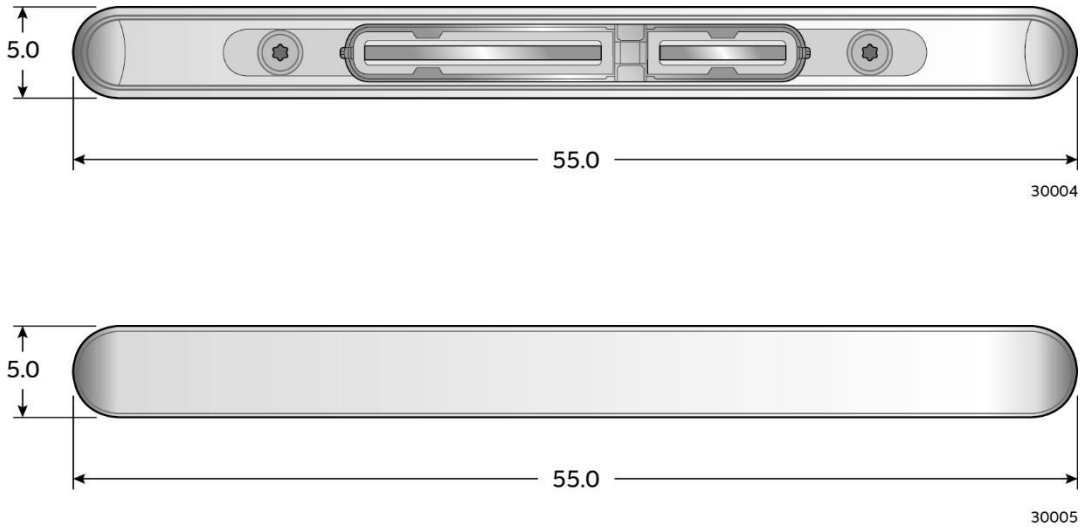

Figure 7. Compute Card Dimensions (Front and Back)

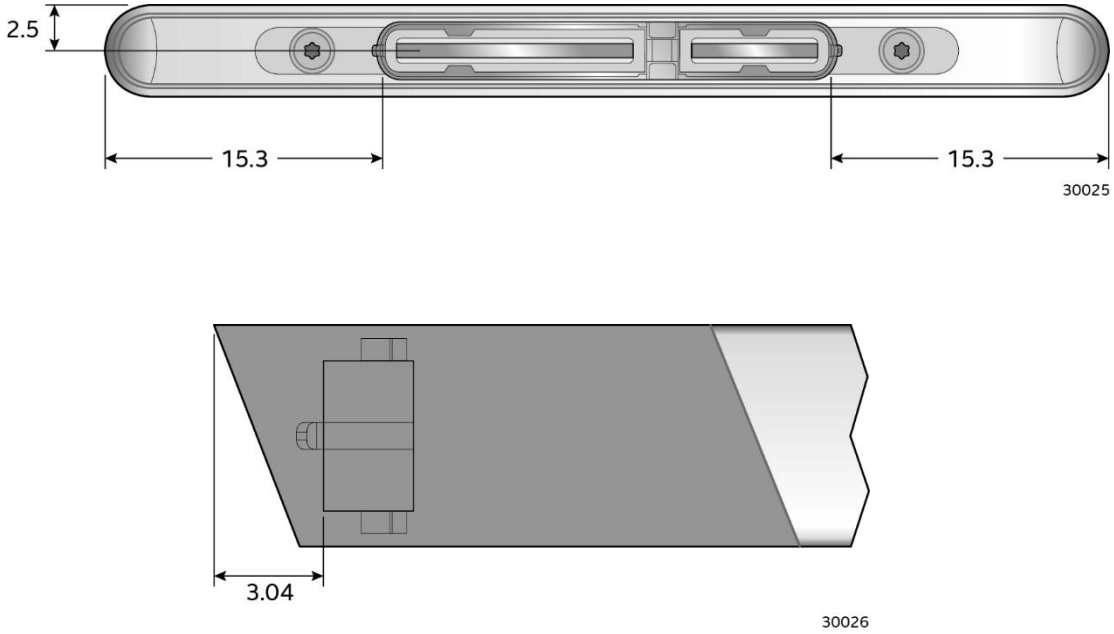

Figure 8. Compute Card Dimensions (Connector)

Table 9. Compute Card Weight Information

Item	Weight
Compute Card only	44.5g
Compute Cards in 5 pack box	680.4g

2.5 Thermal Considerations

The fundamental design of the Intel® Compute Card relies on the installed device for proper cooling and due to the wide variety of potential environmental conditions, no specific cooling design details are provided in this document. The following addresses the primary considerations for proper cooling of the Compute Card.

Power is dissipated from both faces of the Compute Card, however the bottom surface is in direct contact with the CPU and as such receives the majority of the total power. Table 10 lists different power measurements taken on the Compute Card.

Table 10. Power Usage

Type	Full Load	4K Video	4K Streamed Video
Input Power	11.73 W	5.51 W	7.49 W
CPU Package Power	5.95 W	3.78 W	4.56 W
Other Components Power	5.78 W	1.73 W	2.93 W

Direct conductive contact with the Compute Card surfaces will typically provide the best overall heat dissipation, however it is possible to achieve desirable performance levels with convection only cooling. With the use of either conductive or convective cooling, skin temperatures must be taken into consideration. The Compute Card is capable of operating within all critical component temperature specifications while producing surface skin temperatures that may violate typical safety guidelines or requirements. Acceptable skin temperature limits vary with intended use conditions. Reference IEC 60950-1 INFORMATION TECHNOLOGY EQUIPMENT - SAFETY for guidance.

Surface temperatures based on actual use of the Compute Card shown in Table 11 are recommended.

Table 11. Skin Temperature Recommendations

Usage	Temperature
The Compute Card can be removed from the device by a user	55 °C
The Compute Card is enclosed in a device and cannot be removed by a user	70 °C

2.6 Reliability

The Mean Time Between Failures (MTBF) prediction is calculated using component and subassembly random failure rates. The MTBF prediction is used to estimate repair rates and spare parts requirements. The MTBF for the Intel® Compute Card is 53,708 hours.

2.7 Environmental

Table 12 lists the environmental specifications for the Intel® Compute Card.

Table 12. Environmental Specifications

Parameter	Specification		
Temperature			
Non-Operating	-40 °C to +60 °C		
Operating	Ambient operating temperature limitations are a function of the slot design and as such a specific number cannot be provided		
Shock			
Unpackaged	80cm drop		
Packaged	Half sine 2 millisecond		
	Product Weight (pounds)	Free Fall (inches)	Velocity Change (inches/s²)
	<20	36	167
	21-40	30	152
	41-80	24	136
	81-100	18	118
Vibration			
Unpackaged	5 Hz to 20 Hz: 0.01 g² Hz sloping up to 0.02 g² Hz		
	20 Hz to 500 Hz: 0.02 g² Hz (flat)		
Packaged	5 Hz to 40 Hz: 0.015 g² Hz (flat)		

1 The operating and non-operating environment must avoid condensing humidity.

3 Overview of BIOS Features

3.1 Introduction

The Intel® Compute Card uses an Intel® BIOS that is stored in the Serial Peripheral Interface Flash Memory (SPI Flash) and can be updated using a disk-based program. The SPI Flash contains the BIOS Setup program, POST, the PCI auto-configuration utility, and Plug and Play support. The initial production BIOSs are identified as MKKBLY35.86A or MKKBLi5v.86A.

The BIOS Setup program can be used to view and change the BIOS settings for the computer, and to update the system BIOS. The BIOS Setup program is accessed by pressing the <F2> key after the Power-On Self-Test (POST) memory test begins and before the operating system boot begins.

3.2 BIOS Flash Memory Organization

The Serial Peripheral Interface Flash Memory (SPI Flash) includes:

- 128 Mb (16384 KB) flash memory device for CD1IV128MK
- 64 Mb (8192 KB) flash memory device for CD1M3128MK

3.3 System Management BIOS (SMBIOS)

SMBIOS is a Desktop Management Interface (DMI) compliant method for managing computers in a managed network.

The main component of SMBIOS is the Management Information Format (MIF) database, which contains information about the computing system and its components. Using SMBIOS, a system administrator can obtain the system types, capabilities, operational status, and installation dates for system components. The MIF database defines the data and provides the method for accessing this information. The BIOS enables applications such as third-party management software to use SMBIOS. The BIOS stores and reports the following SMBIOS information:

- BIOS data, such as the BIOS revision level
- Fixed-system data, such as peripherals, serial numbers, and asset tags
- Resource data, such as memory size, cache size, and processor speed
- Dynamic data, such as event detection and error logging

Non-Plug and Play operating systems require an additional interface for obtaining the SMBIOS information. The BIOS supports an SMBIOS table interface for such operating systems. Using this support, an SMBIOS service-level application running on a non-Plug and Play operating system can obtain the SMBIOS information. Additional information can be found in the BIOS under the Additional Information header under the Main BIOS page.

3.4 Legacy USB Support

Legacy USB support enables USB devices to be used even when the operating system's USB drivers are not yet available. Legacy USB support is used to access the BIOS Setup program, and to install an operating system that supports USB. By default, Legacy USB support is set to Enabled. In order to boot to a USB device, the Compute Card must be plugged into a compatible device with USB ports.

Legacy USB support operates as follows:

1. When you apply power to the computer, legacy support is disabled.
2. POST begins.
3. Legacy USB support is enabled by the BIOS allowing you to use a USB keyboard to enter and configure the BIOS Setup program and the maintenance menu.
4. POST completes.
5. The operating system loads. While the operating system is loading, USB keyboards and mice are recognized and may be used to configure the operating system. (Keyboards and mice are not recognized during this period if Legacy USB support was set to Disabled in the BIOS Setup program.)
6. After the operating system loads the USB drivers, all legacy and non-legacy USB devices are recognized by the operating system, and Legacy USB support from the BIOS is no longer used.

3.5 BIOS Updates

The BIOS can be updated using either of the following utilities, which are available on the Intel® World Wide Web site:

- Intel® Express BIOS Update Utility, which enables automated updating while in the Windows environment. Using this utility, the BIOS can be updated from a file on a hard disk, a USB drive (a flash drive or a USB hard drive), or a CD-ROM, or from the file location on the Web.
- Intel® F7 switch during POST allows a user to select where the BIOS .bio file is located and perform the update from that location/device.

All utilities verify that the updated BIOS matches the target system to prevent accidentally installing an incompatible BIOS.

NOTE

Review the instructions distributed with the upgrade utility before attempting a BIOS update. The Compute Card must be plugged into a compatible device in order to update the BIOS.

For information about	Refer to
BIOS update instructions	http://www.intel.com/content/www/us/en/support/boards-and-kits/intel-compute-card/000023859.html

3.5.1 Language Support

The BIOS Setup program and help messages are supported in US English. Check the Intel web site for support.

3.6 BIOS Recovery

It is unlikely that anything will interrupt a BIOS update; however, if an interruption occurs, the BIOS could be damaged. Table 13 lists the drives and media types that can and cannot be used for BIOS recovery. The BIOS recovery media plugged into a compatible device does not need to be made bootable.

Table 13. Acceptable Drives/Media Types for BIOS Recovery

Media Type (Note)	Can be used for BIOS recovery?
Hard disk drive (connected to USB)	Yes
CD/DVD drive (connected to USB)	Yes
USB flash drive	Yes

NOTE

Supported file systems for BIOS recovery:

- NTFS (sparse, compressed, or encrypted files are not supported)
- FAT32
- FAT16
- FAT12
- ISO 9660

For information about	Refer to
BIOS recovery	http://www.intel.com/content/www/us/en/support/boards-and-kits/intel-compute-card/000023860.html

3.7 Boot Options

In the BIOS Setup program, the user can choose to boot from local storage or removable storage. The default setting is for the local storage to be the first boot device. For removable storage use the Compute Card must be plugged into a compatible device.

3.7.1 Booting Without Attached Devices

For use in embedded applications, the BIOS has been designed so that after passing the POST, the operating system loader is invoked even if the following devices are not present in a compatible device:

- Video display
- Keyboard
- Mouse

3.7.2 BIOS POST Hotkeys

The following hot keys are supported during boot when the Compute Card is plugged into a compatible device with a keyboard attached to the device.

[F2] Enter BIOS Setup

[F7] Update BIOS

[F10] Enter Boot Menu

3.7.3 Changing the Default Boot Device During POST

When the Compute Card is plugged into a compatible device with a keyboard attached to the device, pressing the <F10> key during POST causes a boot device menu to be displayed. This menu displays the list of available boot devices. Table 14 lists the boot device menu options.

Table 14. Boot Device Menu Options

Boot Device Menu Function Keys	Description
<↑> or <↓>	Selects a default boot device
<Enter>	Exits the menu, and boots from the selected device
<Esc>	Exits the menu and boots according to the boot priority defined through BIOS setup

3.7.4 Power Button Menu

The Power Button Menu is accessible via the following sequence when the Compute Card is plugged into a compatible device that has a power button:

1. System is in S4/S5
2. User pushes the power button and holds it down. Hold the button for 3 seconds, then release the button immediately
3. If the power button is held for longer than 3 seconds the user make invoke the 4-second shutdown override

If this boot path is taken, the BIOS will use default settings, ignoring settings in NVRAM or setup where possible. At the point where Setup Entry/Boot would be in the normal boot path, the BIOS will display the following prompt and wait for a keystroke:

[ESC] Normal Boot

[3] Reset Intel® AMT/Standard Manageability to default factory settings

[4] Clear Trusted Platform Module (Warning: Data encryption with the TPM will no longer be accessible if the TPM is cleared)

[F2] Intel BIOS

[F4] BIOS Recovery

[F7] Update BIOS

[F10] Enter Boot Menu

NOTE

Keys [3] above will only be available on Compute Card CD1IV128MK.

3.7.5 BIOS Error Messages

Table 15 lists the error messages and provides a brief description of each. The Compute Card must be plugged into a compatible device with a display attached in order to view the below messages.

Table 15. BIOS Error Messages

Error Message	Explanation
CMOS Battery Low	The battery may be losing power.
CMOS Checksum Bad	The CMOS checksum is incorrect. CMOS memory may have been corrupted. Run Setup to reset values.
CMOS Time and Data Not Set	The data and time are not set in CMOS. Set the correct time and data in BIOS Setup.
No Boot Device Available	System did not find a device to boot.
Compute Card Thermal Sensor Failure	The thermal sensor in the Compute Card to measure skin temperature is not functioning and may not provide temperature data to the slot device.
Processor Thermal Trip	The processor has exceeded a safe operating temperature which caused the system to shut down.