CEC1702
Silicon Errata and Data Sheet Clarification

TABLE 1: SILICON IDENTIFICATION

Part Number	Silicon Identifier	Functional Revision C	Functional Revision E	Functional Revision F
CEC1702	Device ID(1)	31h	31h	31h
	Revision ID for Silicon Revision(2)	82h	84h	85h
	PIS(3) Version/Revision	B1	B2	B2

Note 1: The Device ID is visible as an 8-bit number at Plug and Play Configuration Index 20h.
2: The HW Revision Number is visible as an 8-bit number at Plug and Play Configuration Index 21h.
3: Product Identification System (PIS) is defined in the Product Data Sheet.

TABLE 2: SILICON ISSUE SUMMARY

Module	Feature	Item Number	Issue Summary	Affected Revisions (1)	Affected Revisions (1)	Affected Revisions (1)
				C	E	F
SMB Controller	SMB Master	1.	SMBus Master Controller violates Bus Idle Time between STO and STA in Byte mode only	X	X	X
JTAG Pins	Pins	2.	GPIO145 & GPIO146 input disabled in SWD mode	X	X	X
ROM API’s	ROM API’s	3.	Some API’s were removed		X	X
Boot ROM	Boot ROM	4.	The Boot ROM may not successfully load Application Code.	X	X	
VBAT	VBAT	5.	High I_{BAT} current on coin cell insertion.	X	X	X

Note 1: Only those issues indicated in the last column apply to the current silicon revision.

Silicon Errata Issues

1. Module: SMBus 2.0 Host Controller

DESCRIPTION

SMBus Master Controller violates Bus Idle Time between STO and STA in Byte mode only. This issue only occurs in a multi-master environment.

Under firmware control, it is possible to generate a new command on the bus before the Bus Idle time expires, thereby violating the SMBus Idle time.

END USER IMPLICATIONS

The SMBus Master Controller may generate a START condition too soon. The two consequences of this scenario are that another master will issue a transaction that will get corrupted, which is handled by the lost arbitration mechanism, or the CEC1702 master will unfairly claim the bus too often.

Work Around

There are two solutions:

a) Use the Network Layer instead of Byte mode. This anomaly does not apply to the SMBus Network Layer operation.

b) If firmware polls the nBB bit to indicate not busy before asserting the PIN bit and writing the data register, the SMBus Controller will not violate the Bus Idle time.

2. Module: GPIO145 and GPIO146 Inputs Disabled When JTAG Enabled

DESCRIPTION

GPIO145 and GPIO146 inputs are disabled when JTAG enabled and the JTAG debugger is connected in both 4-wire JTAG mode and 2-wire SWD mode.

END USER IMPLICATIONS

- Cannot use SMB09 when JTAG is enabled and JTAG debugger is connected if device is configured for 2-wire SWD test mode.
- Cannot use GPIO145 and GPIO146 inputs when JTAG is enabled and JTAG debugger is connected if device is configured for 2-wire SWD test mode.

Work Around

None.

3. Module: ROM API's

DESCRIPTION

Some APIs have been removed from the Functional Revision E devices.

The "version" API return value can be used to determine the version number of the ROM that corresponds to the functional revision of the device as shown in Table 3 below:

TABLE 3: ROM VERSION NUMBER

Functional Revision	Version API Return Value	Boot ROM Revision	ROM API Manual
C	0x00280032	A1	MEC2016_Rom_A1_API_Manual.docx
E	0x00400232	B0	MEC2016_Rom_B0_API_Manual.pdf
F	0x00450032	B1	MEC2016_Rom_B0_API_Manual.pdf

The APIs in the Table 4 have been removed from the Functional Revision E devices. Note that all APIs from the Functional Revision C devices, except for those in the Table 4, are present in the Functional Revision E devices.

The replacement for the removed API is shown in the Table 4, if applicable. Please refer to the appropriate ROM API Manual for the device. Note that the replacement API may not be a direct replacement; please refer to the manual for the correct usage of each API.

TABLE 4: REPLACEMENT API'S

No	API in Functional Revision C	Replacement API in Functional Revision E
1	sha_init	api_sha_direct_init
2	sha_update	api_sha_direct_update
3	sha_final	api_sha_direct_finalize
4	sha12_init	api_sha256_init
5	sha12_update	api_sha256_update
6	sha12_finalize	api_sha256_finalize
7	sha35_init	api_sha512_init
8	sha35_update	api_sha512_update

TABLE 4: REPLACEMENT API'S (CONTINUED)

No	API in Functional Revision C	Replacement API in Functional Revision E
9	sha35_finalize	api_sha512_finalize
10	pke_write_scm32	api_pke_copy_to_scm2
11	rsa_load_key	api_pke_rsa_load_key
12	rsa_load_crt_params	api_pke_rsa_load_crt_key
13	rsa_encrypt	api_pke_rsa_crypt
14	rsa_decrypt	api_pke_rsa_crypt
15	qmspi_cfg_spi_cmd	None. Refer to the QMSPI source code for example QMSPI accesses.
16	qmspi_read_fifo	None. Refer to the QMSPI source code for example QMSPI accesses.
17	qmspi_start_dma	None. Refer to the QMSPI source code for example QMSPI accesses.

END USER IMPLICATIONS

- The APIs listed in the Table 4 above are not present in the Functional Revision E devices. The replacement for the removed API is shown in the Table 4, if applicable. Refer to the appropriate ROM API Manual for the device.

Work Around

Use the version API as described above in Table 3 to determine the version of the device, if required. Use the Replacement APIs in the Table 4 above for functional revision E parts.

4. Module: Boot ROM

DESCRIPTION

The Boot ROM may generate a Load Failure condition for a limited number of valid images in error. If the failure occurs on the TAG0 image, the Boot ROM will attempt to load the TAG1 image. If the failure occurs on the TAG1 image, the Boot ROM will go to the Load Failure exit state.

This error has been found on a very small subset of images and is dependent on a deterministic synchronous timing event that is dependent on image size and SPI Flash acquisition timing.

Identifying Timing Failure: If this timing failure occurred, then the value "0x0D21" will be in the ROM Event log. Please refer to Boot ROM Addendum for Boot ROM Event Log information.

END USER IMPLICATIONS

- Boot may fail when using different SPI frequency or SPI mode for the same payload.

Work Around

Recommendations to solve this problem

- The firmware image is padded to be 64 byte aligned. Pad image with an additional 64 bytes to change size of image.
- Total image (Application binary + trailer for encryption and \ or authentication, if enabled) to be loaded from SPI, should reside only in code SRAM space.
- For larger SRAM devices, for all SPI frequencies, recommended safest SPI operation is QUAD mode.
- If you still sees the Boot code failure, please get in touch with the Microchip support team.

5. Module: VBAT

DESCRIPTION

There could be a high I_{BAT} current on new coin cell insertion. During initial VBAT power rising, the VBAT circuit can enter a high current state causing a voltage drop across the 1K UL resistor.

END USER IMPLICATIONS

- Under these conditions, the VBAT power on can stall in this high current state, with the VBAT on device pin between 0.7 and 1.2V.

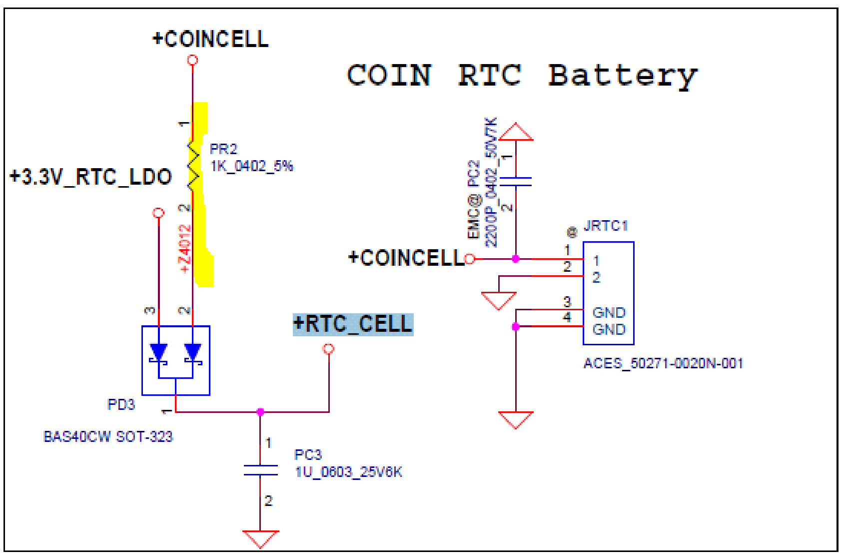
Work Around

When inserting the coin-cell follow the below procedure

Insert the coin cell and then apply VTR (i.e +3VALW). This enables VBAT low-power operation. A high I_{BAT} will not return on subsequent VTR power cycles.

Referring to the RTC Battery circuit shown in Figure 1, applying VTR via the +3.3V_RTC_LDO signal, powers RTC_Cell (which is connected to VBAT) directly (without a series 1k resistor and hence no IR drop from the applied VTR), raising VBAT (RTC_Cell) to greater than 2.0 volts. This takes VBAT out of the "high current" region discussed above enabling normal VBAT low power operation.

FIGURE 1: HIGH IBAT CURRENT DURING COIN CELL INSERTION



Data Sheet Clarifications

The following typographic corrections and clarifications are to be noted for the latest version of the device data sheet.

Note:	Corrections are shown in **bold**. Where possible, the original bold text formatting has been removed for clarity.

TABLE 5: DATA SHEET CLARIFICATION SUMMARY

Module	Item Number	Issue Summary
WDT	1.	WDT_STATUS bit is Reserved
EFUSE	2.	The ATE Mode bit is located in EFUSE Byte 35
PIS	3.	Version/Revision B modified
WDT	4.	WDT_Count is reset on RESET_SYS
WDT	5.	WDT Event Count Register is not programmed by Boot ROM, but needs to be programmed by application firmware.
PCR	6.	VBAT_RESET_STATUS in Power Clock and Reset block indicates status of RESET_VBAT
PCR	7.	JTAG_RESET_STATUS in Power Clock and Reset block is replaced with JTAG_RST# and indicates current value of JTAG_RST# pin
PCR	8.	Wake Only interrupt example and explanation
Pin Configuration	9.	In Figure14-2, nSYS_RST should be read as RESET_SYS
PCR	10.	VTR_RESET_STATUS bit Power Clock and Reset block is renamed to RESET_SYS_STATUS
Electrical Specification	11.	In Table 38-11: VTR SUPPLY CURRENT, I_VTR, EC_CLK is gated Off for Light Sleep condition.
RC_ID	12.	TABLE 25-2, TABLE 25-3, TABLE 25-4 are Sample RC values for 24MHz system clock and CLOCK_SET field in the RC_ID Control Register is set to ‘1’

1. Module: WDT

This section clarifies which WDT status bit must be used for detecting watchdog timer events.

WDT TIMER EVENTS

The WDT_STATUS bit documented in the WDT Control register is a Reserved bit and cannot be used to detect watchdog timer events.

Bit[5] WDT located in the Power-Fail and Reset Status register in the VBAT Register Bank must be used as the WDT Status bit.

2. Module: EFUSE

This section clarifies where the ATE Mode bit is located in the EFUSE block.

ATE MODE BIT IS LOCATED AT BYTE 35 BIT 7 OF EFUSE MODULE

The ATE Mode bit is located in EFUSE Byte 35 Bit[7]:

ATE Mode

1 = Normal

0 = ATE Mode

If ATE Mode bit has not been programmed (i.e., blank parts) then the Boot ROM will perform the following steps:

1. Lock Secure ROM Key
2. Enable 4-wire JTAG
3. Halt Processor

If ATE Mode bit is set, Boot ROM will initialize the device and then begin the SPI Port Selection process defined in the Boot ROM document.

3. Module: Product Information System (PIS)

This section modifies entry Version/Revision B.

B# B = UNPROVISIONED OTP - CUSTOMER NEEDS TO PROVISION, # = VERSION REVISION NUMBER

Version/Revision: B# B = Unprovisioned OTP, # = Version Revision Number

4. Module: WDT

This section clarifies which Reset clears the WDT Count.

WDT COUNT RESET

The WDT_COUNT documented in the WDT Count Register is reset by RESET_SYS and not RESET_SYS_nWDT.

5. Module: WDT

This section clarifies programming of WDT EVENT COUNT Register.

WDT EVENT COUNT REGISTER IS NOT PROGRAMMED BY BOOT ROM

The WDT Event Count Register in EC Subsystem block with offset address 28h has following definition. This field is cleared to 0 on a reset triggered by the main power on reset, but not on a reset triggered by the Watchdog Timer. This field may be used by application firmware to monitor WDT activity. The application firmware must manually increment this register to indicate the number of times a WDT event fired since the chip was last reset by a RESET_SYS_nWDT event.

The recommended procedure is as follows:

1. Check WDT bit located in Power-Fail and Reset Status Register. If WDT = 1, first clear WDT status bit in Power-Fail and Reset Status Register and then increment WDT Event Count register.
2. Enable WDT using the WDT Activation Mechanism defined in Watchdog Timer (WDT) datasheet chapter

6. Module: PCR

The VBAT_RESET_STATUS (bit 5) in PCR Power Reset Status Register indicates RESET_VBAT status and not RESET_VTR.

7. Module: PCR

JTAG_RESET_STATUS bit in PCR Power Reset Status Register is renamed to JTAG_RST# and indicates the current value of JTAG_RST# pin.

JTAG RESET STATUS IS REPLACED WITH JTAG_RST# AND INDICATES STATUS OF JTAG_RST# PIN

The JTAG_RESET_STATUS (bit 7) in PCR Power Reset Status Register is replaced with the JTAG_RST# and indicates the status of JTAG_RST# pin. This is a Read Only bit.

0 = JTAG_RST# pin is low

1 = JTAG_RST# pin is high

Note:	This bit always reflects the state of the JTAG_RST# pin even when Boundary Scan Enabled.

8. Module: PCR

This section clarifies Wake-Only Events in Section 5.7.3.1 and gives an example and explanation.

WAKE-ONLY INTERRUPT IN GIRQ22 JUST GENERATES CLOCK FOR THE RESPECTIVE BLOCK AND DO NOT WAKE THE PROCESSOR

The Wake-Only Events and interrupts are responsible for waking up the respective blocks from where the Event or interrupt becomes active, but will not enable the clock to the processor.

For example, when RSMRST is high and there is a desire to wake from an ESPI cycle, GIRQ22[9] is the correct wake source to use. When Chip is asleep and there is a ESPI cycle, the falling edge of the CS will cause the chips clock to turn on the ESPI block, but not the processor itself. Upon conclusion of the ESPI cycle, if no ESPI interrupt was generated (i.e. most cycles), then the clock to the ESPI block will go off, and the chip will go back to sleep. If the ESPI cycle creates an interrupt to the processor (i.e. downstream wire or downstream OOB packet for example), then an processor interrupt will be generated if enabled and the clock will remain on and the processor can service the interrupt and the processor can put the chip back to sleep when it has completed its work.

Note:	The ESPI Reset itself is NOT a wake event. If wake from ESPI reset is required, then the GPIO interrupt for the ESPI reset pin can be used as a wake event.

9. Module: Pin Configuration

nSYS_RST in FIGURE 14-2 should be read as RESET_SYS.

10. Module: PCR

The VTR_RESET_STATUS (bit 6) in PCR Power Reset Status Register is replaced with RESET_SYS_STATUS and indicates the status of RESET_SYS. This R/WC bit is set any time the RESET_SYS signal is asserted.

11. Module: Electrical Specification

POWER CONSUMPTION IN LIGHT SLEEP

Table 38-11, VTR SUPPLY CURRENT, I_VTR incorrectly indicates the EC_CLK frequency is 12MHz in Light Sleep. The EC_CLK is gated Off (0 MHz) in Light sleep condition.

12. Module: RC_ID

Section 25.11 Time Constants in CEC1702 Data sheet incorrectly states following statement “In the following tables, the CLOCK_SET field in the RC_ID Control Register is set to ‘0’, so the time base for measuring the rise time is 48MHz, the speed of the system clock”. The correct speed of the system clock is 24MHz for the count value listed in Table 25-2,Table 25-3 and Table 25-4.

SYSTEM CLOCK USED TO MEASURE COUNT IS 24MHZ

The correct statement for Section 25.11 is listed below.

“This section lists a set of R and C values which can be connected to the RC_ID pin. Note that rise time generally follow RC time Tau. Firmware should use the Max and Min Counts in the tables to create quantized states.

In the following tables, the CLOCK_SET field in the RC_ID Control Register is set to ‘1’, so the time base for measuring the rise time is 24MHz, the speed of the system clock. All capacitor values are ±10% and all resistor values are ±5%.

Minimum and maximum count values are suggested ranges, calculated to provide reasonable margins around the nominal rise times. Rise times have been confirmed by laboratory measurements.”

APPENDIX A: DOCUMENT REVISION HISTORY

REVISION	DESCRIPTION
DS80000726F (10-14-19)	Added Silicon Revision F in Table 1, Table 2 and Table 3. Added Errata # 5. - High I_{BAT} current on coin cell insertion.
DS80000726E (03-07-19)	Added Silicon Summary Issue # 4. - The Boot ROM may not successfully load Application Code.
	Removed Silicon Summary Issue #4. - Some QMSPI APIs do not function correctly and merged the API's with Silicon Summary Issue # 3. - Some API's were removed.
DS80000726D (04-04-18)	Added Data Sheet Clarification # 12. - TABLE 25-2, TABLE 25-3, TABLE 25-4 are Sample RC values for 24MHz system clock and CLOCK_SET field in the RC_ID Control Register is set to '1'.
	Added Data Sheet Clarification # 4. - WDT_Count is reset on RESET_SYS. Added Data Sheet Clarification # 5. - WDT Event Count Register is not programmed by Boot ROM, but needs to be programmed by application firmware. Added Data Sheet Clarification # 6. - VBAT_RESET_STATUS in Power Clock and Reset block indicates status of RESET_VBAT. Added Data Sheet Clarification # 7. - JTAG_RESET_STATUS in Power Clock and Reset block indicates should be JTAG_RST#. Added Data Sheet Clarification # 8. - Wake Only interrupt example and explanation. Added Data Sheet Clarification # 9. - In Figure21-2, nSYS_RST should be read as RESET_SYS. Added Data Sheet Clarification # 10. - VTR_RESET_STATUS bit Power Clock and Reset block indicates is renamed to RESET_SYS_STATUS. Added Data Sheet Clarification # 11. - In Table 38-11: VTR SUPPLY CURRENT, I_VTR, EC_CLK is gated off in Light Sleep condition. Added Silicon Summary Issue # 3. - Some API's were removed. Added Silicon Summary Issue #4. - Some QMSPI APIs do not function correctly.
DS80000726C (01-11-18)	Added Data Sheet Clarification # 2. - The ATE Mode bit is located in EFUSE Byte 35. Added Data Sheet Clarification # 3. - Version/Revision B modified.
DS80000726B (10-05-17)	Functional Revision E added for reference.
DS80000726A (01-30-17)	Initial release

THE MICROCHIP WEB SITE

Microchip provides online support via our WWW site at www.microchip.com. This web site is used as a means to make files and information easily available to customers. Accessible by using your favorite Internet browser, the web site contains the following information:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQ), technical support requests, online discussion groups, Microchip consultant program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

CUSTOMER CHANGE NOTIFICATION SERVICE

Microchip's customer notification service helps keep customers current on Microchip products. Subscribers will receive e-mail notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, access the Microchip web site at www.microchip.com. Under "Support", click on "Customer Change Notification" and follow the registration instructions.

CUSTOMER SUPPORT

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Field Application Engineer (FAE)
- Technical Support

Customers should contact their distributor, representative or field application engineer (FAE) for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in the back of this document.

Technical support is available through the web site at: http://www.microchip.com/support

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as "unbreakable."

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

ISBN: 9781522451242

For information regarding Microchip's Quality Management Systems, please visit www.microchip.com/quality.

Worldwide Sales and Service

AMERICAS

Corporate Office
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-792-7200
Fax: 480-792-7277
Technical Support:
http://www.microchip.com/support
Web Address:
www.microchip.com

Atlanta
Duluth, GA
Tel: 678-957-9614
Fax: 678-957-1455

Austin, TX
Tel: 512-257-3370

Boston
Westborough, MA
Tel: 774-760-0087
Fax: 774-760-0088

Chicago
Itasca, IL
Tel: 630-285-0071
Fax: 630-285-0075

Dallas
Addison, TX
Tel: 972-818-7423
Fax: 972-818-2924

Detroit
Novi, MI
Tel: 248-848-4000

Houston, TX
Tel: 281-894-5983

Indianapolis
Noblesville, IN
Tel: 317-773-8323
Fax: 317-773-5453
Tel: 317-536-2380

Los Angeles
Mission Viejo, CA
Tel: 949-462-9523
Fax: 949-462-9608
Tel: 951-273-7800

Raleigh, NC
Tel: 919-844-7510

New York, NY
Tel: 631-435-6000

San Jose, CA
Tel: 408-735-9110
Tel: 408-436-4270

Canada - Toronto
Tel: 905-695-1980
Fax: 905-695-2078

ASIA/PACIFIC

Australia - Sydney
Tel: 61-2-9868-6733

China - Beijing
Tel: 86-10-8569-7000

China - Chengdu
Tel: 86-28-8665-5511

China - Chongqing
Tel: 86-23-8980-9588

China - Dongguan
Tel: 86-769-8702-9880

China - Guangzhou
Tel: 86-20-8755-8029

China - Hangzhou
Tel: 86-571-8792-8115

China - Hong Kong SAR
Tel: 852-2943-5100

China - Nanjing
Tel: 86-25-8473-2460

China - Qingdao
Tel: 86-532-8502-7355

China - Shanghai
Tel: 86-21-3326-8000

China - Shenyang
Tel: 86-24-2334-2829

China - Shenzhen
Tel: 86-755-8864-2200

China - Suzhou
Tel: 86-186-6233-1526

China - Wuhan
Tel: 86-27-5980-5300

China - Xian
Tel: 86-29-8833-7252

China - Xiamen
Tel: 86-592-2388138

China - Zhuhai
Tel: 86-756-3210040

ASIA/PACIFIC

India - Bangalore
Tel: 91-80-3090-4444

India - New Delhi
Tel: 91-11-4160-8631

India - Pune
Tel: 91-20-4121-0141

Japan - Osaka
Tel: 81-6-6152-7160

Japan - Tokyo
Tel: 81-3-6880- 3770

Korea - Daegu
Tel: 82-53-744-4301

Korea - Seoul
Tel: 82-2-554-7200

Malaysia - Kuala Lumpur
Tel: 60-3-7651-7906

Malaysia - Penang
Tel: 60-4-227-8870

Philippines - Manila
Tel: 63-2-634-9065

Singapore
Tel: 65-6334-8870

Taiwan - Hsin Chu
Tel: 886-3-577-8366

Taiwan - Kaohsiung
Tel: 886-7-213-7830

Taiwan - Taipei
Tel: 886-2-2508-8600

Thailand - Bangkok
Tel: 66-2-694-1351

Vietnam - Ho Chi Minh
Tel: 84-28-5448-2100

EUROPE

Austria - Wels
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

Denmark - Copenhagen
Tel: 45-4450-2828
Fax: 45-4485-2829

Finland - Espoo
Tel: 358-9-4520-820

France - Paris
Tel: 33-1-69-53-63-20
Fax: 33-1-69-30-90-79

Germany - Garching
Tel: 49-8931-9700

Germany - Haan
Tel: 49-2129-3766400

Germany - Heilbronn
Tel: 49-7131-72400

Germany - Karlsruhe
Tel: 49-721-625370

Germany - Munich
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

Germany - Rosenheim
Tel: 49-8031-354-560

Israel - Ra'anana
Tel: 972-9-744-7705

Italy - Milan
Tel: 39-0331-742611
Fax: 39-0331-466781

Italy - Padova
Tel: 39-049-7625286

Netherlands - Drunen
Tel: 31-416-690399
Fax: 31-416-690340

Norway - Trondheim
Tel: 47-7288-4388

Poland - Warsaw
Tel: 48-22-3325737

Romania - Bucharest
Tel: 40-21-407-87-50

Spain - Madrid
Tel: 34-91-708-08-90
Fax: 34-91-708-08-91

Sweden - Gothenberg
Tel: 46-31-704-60-40

Sweden - Stockholm
Tel: 46-8-5090-4654

UK - Wokingham
Tel: 44-118-921-5800
Fax: 44-118-921-5820