

User Manual

Rev. 1.2

SmartRF[®] CC2420DK: Packet Sniffer for IEEE 802.15.4 and ZigBee

SmartRF[®]

Chipcon AS, Gaustadalléen 21, N-0349 Oslo, Norway. Tel: +47 22 95 85 45, fax: +47 22 95 85 46.
E-mail: support@chipcon.com

Table of contents

1	INTRODUCTION	3
1.1	HARDWARE PLATFORM	3
1.2	SOFTWARE	3
2	USER INTERFACE	4
2.1	MENUS AND TOOLBARS.....	6
2.2	SETUP	6
2.3	SELECT FIELDS	7
2.3.1	<i>Tips</i>	7
2.4	PACKET DETAILS	7
2.5	ADDRESS BOOK	9
2.5.1	<i>Tips</i>	9
2.6	DISPLAY FILTER	10
2.7	TIME LINE	10
3	HELP	11
4	TROUBLESHOOTING	12
5	GENERAL INFORMATION	13
5.1	DOCUMENT HISTORY	13
5.2	DISCLAIMER.....	13
5.3	TRADEMARKS	13
6	ADDRESS INFORMATION	14

1 Introduction

The packet sniffer captures, filters and decodes IEEE 802.15.4 MAC packets, and displays them in a convenient way, with options for filtering and storage to a binary file format.

The packet sniffer also has the optional ability to decode the MAC data frames at the ZigBee Network (NWK) and Application Support Sublayer (APS).

The packet sniffer for CC2420DK is installed separately from SmartRF® Studio, and must be downloaded from our web site. A shortcut will be placed on the Windows "Start menu" after the installation.

1.1 Hardware Platform

The packet sniffer requires a single CC2400EB with a CC2420EM connected to it. The CC2400EB board is connected to the PC through a USB cable (USB version 1.1).

A fast (i.e. modern) computer is required to handle the incoming packets, with a worst-case rate of about 1000 packets per second. The board is able to queue up to 248 packets for USB transfer, thus allowing for shorter periods of high workload for the computer. Media players and other CPU hungry applications should however be shut down before activating the packet sniffer.

The amount of packets that can be stored on the computer depends upon the buffer size, which can be set before the sniffer is started (20 MBs by default = approximately 20000 packets). The sniffer will stop automatically when the buffer runs full, and a message box will pop up.

Figure 1 below shows the data flow for the packet sniffer.

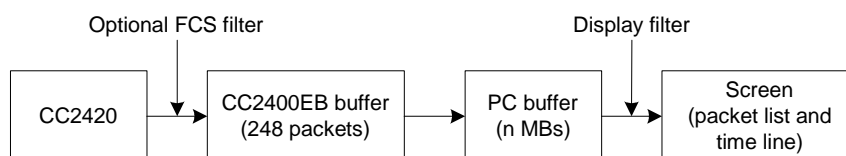


Figure 1. Data flow for the IEEE 802.15.4 / ZigBee packet sniffer

1.2 Software

The firmware that is required for the FPGA and the USB microcontroller, is downloaded automatically when the CC2400EB is connected to the computer.

The following platforms are supported:

- Windows 98
- Windows Me
- Windows 2000
- Windows XP

Please note that the SmartRF® Studio device manager will lock up while the packet sniffer is running.

2 User Interface

The packet sniffer user interface can be divided into two sections:

- At the top; A **packet list**, which displays the various fields of the decoded packets.
- At the bottom; The following six tabs:
 - **Setup**: Selects which evaluation board to use, the packet buffer size (20 MB by default), and the channel to capture packets from.
 - **Select fields**: Select which fields to display in the packet list, including IEEE 802.15.4 MAC and ZigBee NWK and APS layers.
 - **Packet details**: Displays additional packet details (e.g. raw data).
 - **Address book**: Contains all known MAC addresses from the current sniffing session. Addresses can be registered automatically or manually, changed and deleted.
 - **Display filter**: Packet filtering on packet types and addresses (based on the address book entries).
 - **Time line**: Displays a large sequence of packets, about 20 times as many as in the packet list, sorted by either MAC source or destination addresses (based on the address book entries).

The packet sniffer screenshot in Figure 2 shows a successful association in a beacon network with no short address assigned to the device (short address 0xFFFFE). The association response is transmitted indirectly from the coordinator.

The status bar displays the total (unfiltered) number of captured packets, and the current memory buffer status.

Time (us)	Length	Frame control field	Sequence number	Source PAN	Source Address	Superframe specification	GTS fields	LQI	FCS	
+15358 =6250666	13	Type Sec Pnd Ack req Intra PAN BCN 0 0 0 0	0xCA	0xB00B	0xC001	B0 S0 F.CAP BLE Coord Assoc 00 00 15 0 1 1	Len Permit 0 1	124	OK	
+9700 =6260366	21	Type Sec Pnd Ack req Intra PAN CMD 0 0 1 0	0x99	0xB00B	0xC001	0xFFFF	0x0000004722958919	Association request Alt.coord FFD Power Idle RX Sec Alloc addr 0 0 0 0 0 0 1		
+1179 =6261545	5	Type Sec Pnd Ack req Intra PAN ACK 0 0 0 0	0x99					136	OK	
+4479 =6266024	13	Type Sec Pnd Ack req Intra PAN BCN 0 0 0 0	0xCB	0xB00B	0xC001	B0 S0 F.CAP BLE Coord Assoc 00 00 15 0 1 1	Len Permit 0 1	136	OK	
+15358 =6281382	21	Type Sec Pnd Ack req Intra PAN BCN 0 0 0 0	0xCC	0xB00B	0xC001	B0 S0 F.CAP BLE Coord Assoc 00 00 15 0 1 1	Len Permit 0 1	Pending addresses Short: Ext: 0x0000004722958919		
+3943 =6285325	20	Type Sec Pnd Ack req Intra PAN CMD 0 0 1 0	0x9A	0xB00B	0xC001			Data request 224 OK		
+1176 =6286501	5	Type Sec Pnd Ack req Intra PAN ACK 0 0 0 0	0x9A					136	OK	
+2240 =6288741	29	Type Sec Pnd Ack req Intra PAN CMD 0 0 1 0	0xAE	0xB00B	0xC001	0x0000004722958919	0xB00B	0x0000EB0000000014	Association response Short addr Assoc, status 0xFFFF Successful	
+1316 =6290057	5	Type Sec Pnd Ack req Intra PAN ACK 0 0 0 0	0xAE					224	OK	
+6683 =6296740	13	Type Sec Pnd Ack req Intra PAN BCN 0 0 0 0	0xCD	0xB00B	0xC001	B0 S0 F.CAP BLE Coord Assoc 00 00 15 0 1 1	Len Permit 0 1	136	OK	

Setup	Select fields	Packet details	Address book	Display filter	Time line
-------	---------------	----------------	--------------	----------------	-----------

Select CC2420 Evaluation Board:









[0] - Chipcon - CC2400EB (VID=11A0, PID=EB11, DID=2420)

Select packet buffer size: 100 MB Select channel: 0x0B (2405 MHz) Clock multiplier: 1.0

Packet count: 436 Memory usage: 0.4% No overflow

Figure 2. Packet sniffer screenshot

2.1 Menus and Toolbars

Menu	Button	Key	Description
File→Reset...			Empties the packet buffer and the packet list.
File→Open data...			Load packet buffer and address book from file
File→Save data...			Save packet buffer and address book to file
			* Display the tabs at the bottom of the window?
		F5	Start the packet sniffer (does not empty the buffer)
		F6	Pause the packet sniffer
			* Delete all captured packets when starting
			* Enable FCS filtering on the CC2400EB?
Help→PSD format..			A description of packet sniffer data files, which contain raw data from the captured packets.
Help→User Manual			Opens this document in Adobe Acrobat (Reader)
Help→Rev. History			Revision history (bug fixes, new features, etc.)

The application is closed by double-clicking in the top left corner, or single-clicking on the X-symbol in the top right corner.

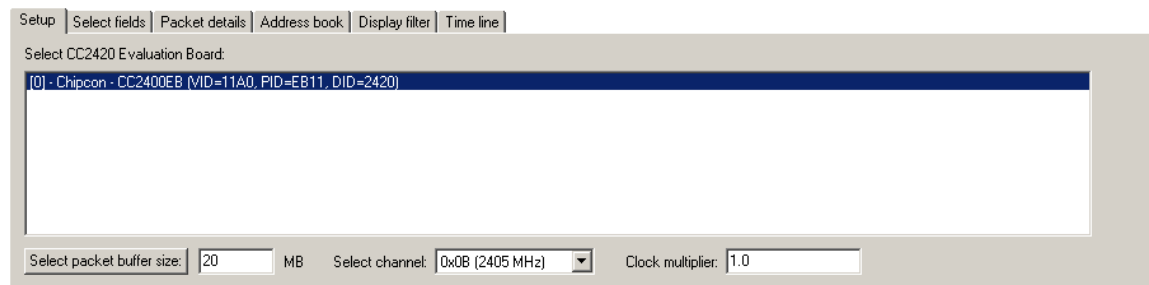
Items marked with a star (*) are saved to Windows registry between each session.

2.2 Setup

The setup tab configures the packet sniffer by selecting:

- Which evaluation board to use
- The size of the packet buffer in megabytes (the default value of 20 MB allows for approximately 20000 packets to be stored). Please note that you must push the select button to change the size.
- Which channel to use (0x0B – 0x1A, 2405 MHz – 2480 MHz).
- A clock multiplier, which allows you to compensate for clock speed differences on the CC2400EB and the hardware running your application.

These selections must all be made before the packet sniffer is started (which is done by pushing the tool bar button, or hitting the F5 key).



The settings entered here are saved to Windows registry between each session.

2.3 Select fields

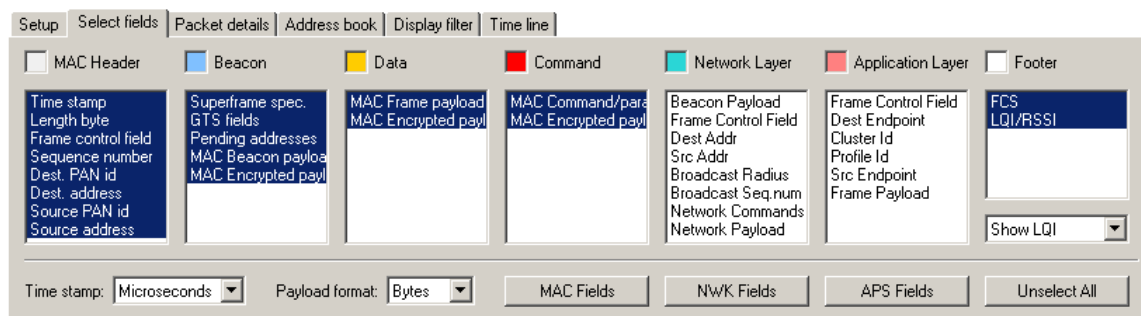
The field selection tab can be used to select which fields to display and which to hide in the packet list control. This feature is particularly useful for low-resolution screens (less than 1024x768).

The time stamp can be displayed in microseconds or milliseconds. The beacon and MAC data payload can be displayed as hex-bytes or as plain-text. In plain-text format all non-printable characters will be replaced by a "*".

The select fields tab also enables decoding of ZigBee Network (NWK) and Application Support Sublayer (APS) fields within MAC layer data frames. Each subfield is sorted into one out of seven color coded categories.

There are three buttons available for selecting all fields within the MAC, NWK and APS layer respectively. There is also one button for unselecting all fields.

Each frame can either be shown with its LQI (ranging from 0x00 to 0xFF) or RSSI (with an approximation to the actual RF level, in dBm).



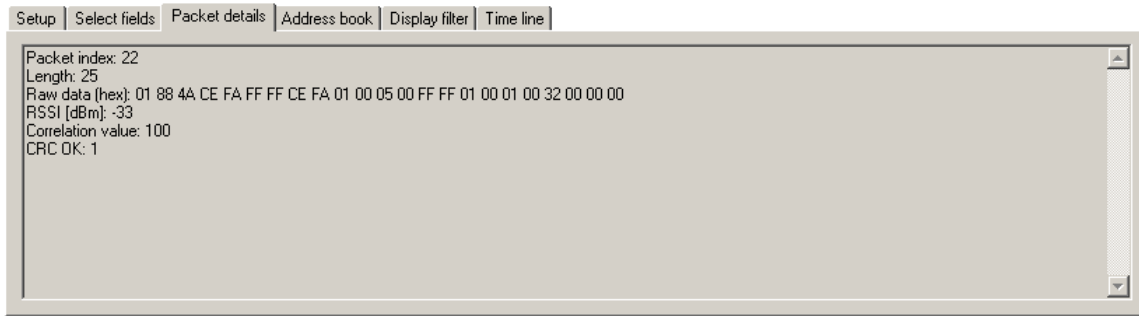
2.3.1 Tips

Extended selection is used to operate the controls:

- To select a range of fields:
 - Click and drag over the fields that should be selected, or....
 - ... select the first field, hold down the "Shift" key, and select the last field.
- To select/unselect a single field:
 - Hold down the "Ctrl" key and click on the field to be toggled.

2.4 Packet details

By double-clicking on a packet in the packet list, additional details, as shown below, will be displayed:

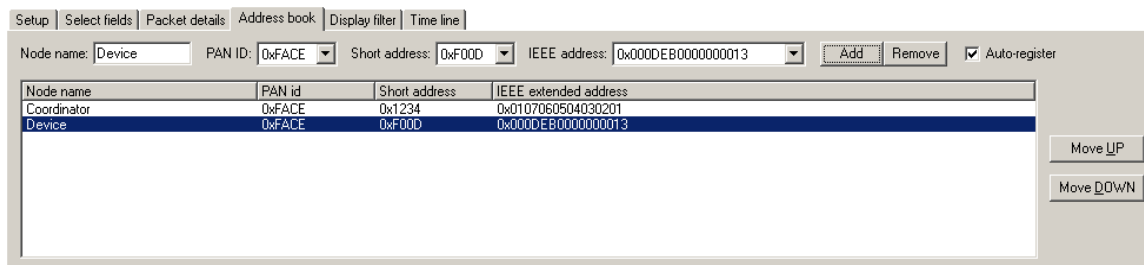


The packet index shows the index for each captured packet, starting with index 0 for the first packet.

The RSSI value is read out of CC2420 and adjusted with -45 to get an approximate value in dBm. The correlation value is equal to the value read out of CC2420. See the CC2420 datasheet for detailed information on the RSSI and correlation values.

2.5 Address book

The address book contains all known MAC addresses from the last session. By selecting "Auto-register" (which is on by default), the packet sniffer will register all addresses automatically and add entries into the address book. Short and extended (64-bit IEEE) addresses will be paired at the reception of association response command packets.



Nodes are added/replaced manually by clicking the "Add" button, or by hitting the "Enter" key while standing in one of the four top fields (Node name, PAN ID, Short address or IEEE address). PAN ID - address duplicates are removed automatically.

Nodes can be removed by clicking the "Remove" button, or by hitting the "Delete" key while standing in the address list.

Nodes can be moved up/down by using the rightmost buttons, or the "Alt + U" and "Alt + D" key combinations.

Please note that some manual editing will be required when:

- There has been a PAN ID conflict.
- A device has left the network, and another device has been given an already used short address (the extended address will be replaced).
- Association response commands have not been detected.

2.5.1 Tips

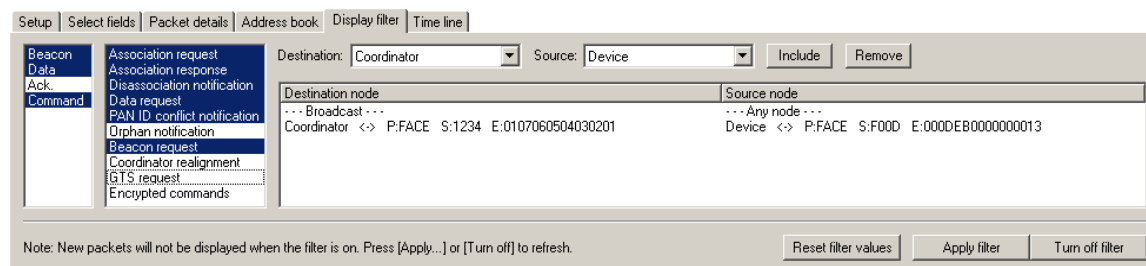
Fast editing of node names can be done using the following procedure:

1. Select the first auto-registered item in the address list
2. Hit "Enter" to copy the data and move to the node name field
3. Enter the new name
4. Hit "Enter" to replace the old entry and move back to the address list
5. Move one line down by using the down arrow.
6. Go to step 2

2.6 Display filter

The MAC display filter, which is applied between the PC packet buffer and the screen, allows for filtering on MAC packet types and MAC addresses:

- MAC Packet types (beacon, data, acknowledgments and MAC commands)
- Individual MAC commands
- Destination and source (based on address book entries)
 - "Any node" includes all packets
 - "Broadcast" includes all packets where the PAN ID or the short address field is 0xFFFF.



Reset, apply the filter, or turn it off by using the three buttons in the bottom right corner.

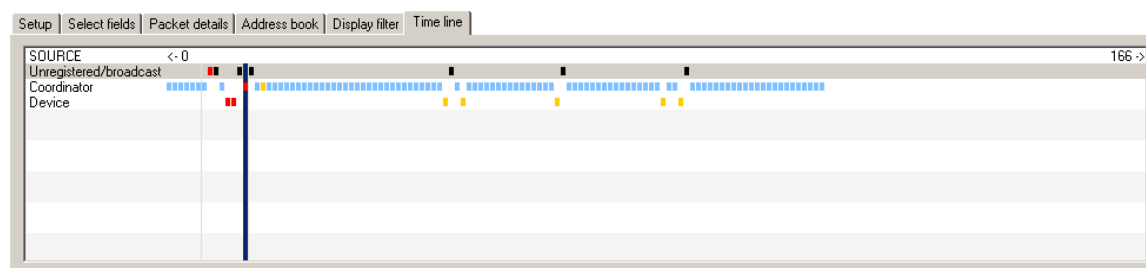
FCS filtering can be done in hardware by pressing the toolbar button. By default, packets with wrong FCS are passed through the filter. FCS filtering must be enabled or disabled before starting the sniffer. Turning it on or off after data has been captured has no effect.

When packets are filtered out, the delta times shown in the Time fields still show the delta time to the previous packet captured, not the previous packet shown.

Note that the display filter only applies at the MAC layer, there are no mechanisms to filter on NWK or APS fields.

2.7 Time line

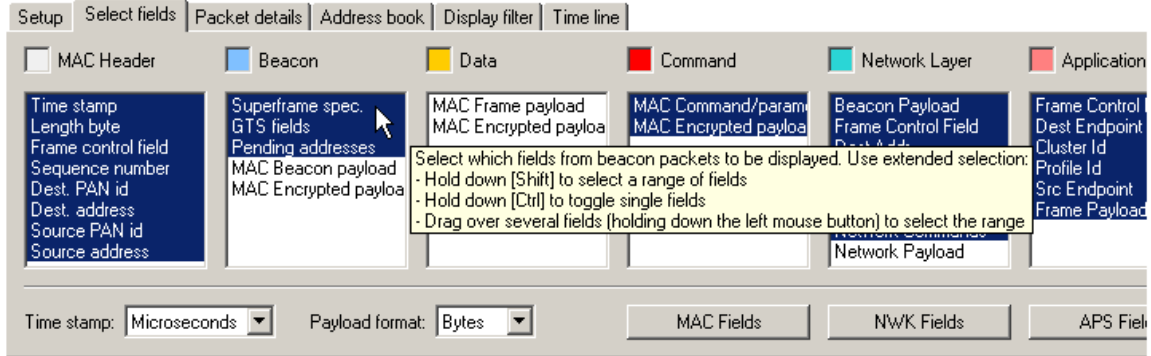
The time line displays all received packets, ordered horizontally by the time of reception and vertically by MAC source or destination address. Selecting a packet from the time line will instantly be reflected in the packet list, and vice versa, thus allowing for efficient navigation in large collections of packets.



Double-click in the left section of the time line to switch between destination and source. Packets are selected by clicking and/or holding down the left mouse button. The time line can be scrolled clicking and holding down the right mouse button (drag).

3 Help

The packet sniffer provides online help through so-called tool-tips. By moving the cursor over a field (e.g. a button or a text field) and holding it in the same position for about half a second, the text will appear in a yellow box slightly below the cursor:



Keyboard and mouse button events will cause the tool-tip to disappear, or not be displayed at all.

4 Troubleshooting

Execute the steps, one by one until the problem is solved.

The evaluation board is not detected (it does not appear in the list box in the Setup tab)

- Make sure that the power cable and the USB cable are connected properly: Press the "Reset" button and wait for the LEDs to start blinking (this confirms that the microcontroller, the EEPROM, the FPGA, and the Windows loader driver work).
- Make sure that the following terminals on the evaluation board are short-circuited:
 - IOC and IIC
 - IOI and III
- Make sure that the CC2420EM has been plugged in, and that the jumpers are set correctly (see the CC2420DK user manual). Press the "Reset" button again.

When pressing the "start button", the sniffer stops immediately (the start button is not grayed out)

- Disconnect the USB cable from the evaluation board, and plug it back in.
- Press the "Reset" button on the evaluation board.
- Disconnect the power cable from all evaluation boards and install the latest version of the packet sniffer.
- Reboot the computer.

The program does not respond

- Press the "Reset" button on the evaluation board.

The packets are not decoded correctly

- Packets with an FCS failure will probably not be parsed correctly (FCS = ERR).
- Make sure that the packet really is correctly formatted (compare the fields with the raw data in the packet details tab).

Weird packets appear in the packet sniffer when I'm not transmitting anything

- CC2420 will try receiving packets down to the RF noisefloor. Sometimes it will also decode packets which are decoded from noise only. These will appear in the packet sniffer. To avoid this, enable FCS filtering in the toolbar.

5 General Information

5.1 Document History

Revision	Date	Description/Changes
1.2	2004-10-15	BUG FIX: Start / stop buttons no longer hang. Prevent starting of sniffer when no RF card is detected. Fixed error in memory usage display. Fixed error in horizontal scrolling in time-line with more than 32768 frames. NEW FEATURE: Decoding of ZigBee Network (NWK) and Application Support Sublayer (APS) frames. Select between RSSI or LQI display in the select .fields dialog. Packet index added to "Packet Details" view. MINOR CHANGE: MAC Sequence Number now displayed in hexadecimal.
1.1	2004-04-27	BUG FIX: Improved the maximum capturing rate. Extended addresses no longer depend on the PAN ID when displayed in the time-line. Several small bug fixes concerned with filtering. Stability problem concerned with the packet time-line (access violation). NEW FEATURE: Hardware buffer overflow is detected. Settings, such as buffer size, radio channel, clock multiplier, and the buttons on the toolbar, are saved to Windows registry. Tool-tips, as in SmartRF Studio for CC2420. Shortcut keys: Press F5 to run and F6 to stop. The current packet buffer can optionally be deleted when the sniffer is started (new toolbar button). A description of the PSD file format has been added to the help menu.
1.0	2003-12-19	Initial release.

5.2 Disclaimer

Chipcon AS believes the information contained herein is correct and accurate at the time of this printing. However, Chipcon AS reserves the right to make changes to this product without notice. Chipcon AS does not assume any responsibility for the use of the described product; neither does it convey any license under its patent rights, or the rights of others. The latest updates are available at the Chipcon website or by contacting Chipcon directly.

To the extent possible, major changes of product specifications and functionality will be stated in product specific Errata Notes published at the Chipcon website. Customers are encouraged to sign up for the Developer's Newsletter for the most recent updates on products and support tools.

When a product is discontinued this will be done according to Chipcon's procedure for obsolete products as described in Chipcon's Quality Manual. This includes informing about last-time-buy options. The Quality Manual can be downloaded from Chipcon's website.

Compliance with regulations is dependent on complete system performance. It is the customer's responsibility to ensure that the system complies with regulations.

5.3 Trademarks

SmartRF[®] is a registered trademark of Chipcon AS. *SmartRF*[®] is Chipcon's RF technology platform with RF library cells, modules and design expertise. Based on *SmartRF*[®] technology Chipcon develops standard component RF circuits as well as full custom ASICs based on customer requirements and this technology.

All other trademarks, registered trademarks and product names are the sole property of their respective owners.

6 Address Information

Web site: <http://www.chipcon.com>
E-mail: wireless@chipcon.com
Technical Support Email: support@chipcon.com
Technical Support Hotline: +47 22 95 85 45

Headquarters:

Chipcon AS
Gaustadalléen 21
NO-0349 Oslo
NORWAY
Tel: +47 22 95 85 44
Fax: +47 22 95 85 46
E-mail: wireless@chipcon.com

US Offices:

Chipcon Inc., Western US Sales Office
19925 Stevens Creek Blvd.
Cupertino, CA 95014-2358
USA
Tel: +1 408 973 7845
Fax: +1 408 973 7257
Email: USsales@chipcon.com

Chipcon Inc., Eastern US Sales Office
35 Pinehurst Avenue
Nashua, New Hampshire, 03062
USA
Tel: +1 603 888 1326
Fax: +1 603 888 4239
Email: eastUSsales@chipcon.com

Sales Office Germany:

Chipcon AS
Riedberghof 3
D-74379 Ingersheim
GERMANY
Tel: +49 7142 9156815
Fax: +49 7142 9156818
Email: Germanysales@chipcon.com

Sales Office Asia :

Chipcon AS
Unit 503, 5/F
Silvercord Tower 2, 30 Canton Road
Tsimshatsui, Hong Kong
Tel: +852 3519 6226
Fax: +852 3519 6520
Email: Asiasales@chipcon.com

Sales Office Korea & South-East Asia:

Chipcon AS
37F, Asem Tower
159-1 Samsung-dong, Kangnam-kuSeoul
135-798 Korea
Tel: +82 2 6001 3888
Fax: +82 2 6001 3711
Email: mailto:KAsiasales@chipcon.com

Sales Office Japan:

Chipcon AS
#403, Bureau Shinagawa
4-1-6, Konan, Minato-Ku,
Tokyo, Zip 108-0075
Japan
Tel: +81 3 5783 1082
Fax: +81 3 5783 1083
Email: Japansales@chipcon.com

Chipcon AS is an ISO 9001:2000 certified company



© 2004 Chipcon AS. All rights reserved.