



nRF Sniffer

User Guide v1.1

1 Overview

The nRF *Bluetooth*® Smart Sniffer is a tool for debugging *Bluetooth* low energy (BLE) applications, picking up (sniffs) every packet between a selected device and the device it is communicating with, even when the link is encrypted. When developing a BLE solution knowing what happens over-the-air between devices can help you isolate and solve any potential issues.

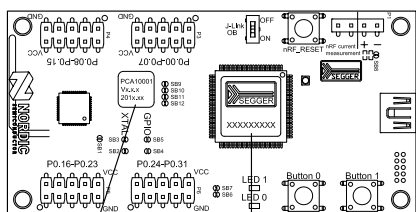
By default, the Sniffer lists nearby BLE devices that are advertising, providing the *Bluetooth* Address and Address type, complete or shortened name, and RSSI.

1.1 Required hardware

To set up the Sniffer you will need one of the following pieces of hardware:

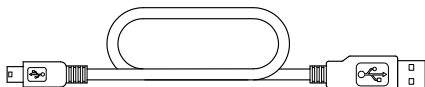
- nRF51822 Evaluation Kit (PCA10001) and a mini USB cable
- nRF51822 Development Kit dongle (PCA10000)

nRF51822 Evaluation Kit board
(PCA10001)



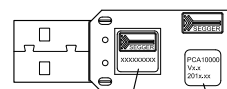
Board name
and version

SEGGER
serial number



Or

nRF51822 Development dongle
(PCA10000)



SEGGER
serial number

Board name
and version

Figure 1 Hardware requirements

1.2 Required software

- Windows 7 or later.
- nRFgo Studio.
- **ble-sniffer-<os>-<version>.exe** and Sniffer plugins and firmware found in **ble-sniffer_<os>_<version>_Sniffer.zip** in the installer folder.
- Wireshark v1.10.1 or later available from <http://www.wireshark.org/>. Download and install to the default directory. Wireshark is a free software tool that captures wireless traffic and reproduces it in a readable format.

1.3 Writing conventions

This user guide follows a set of typographic rules that makes the document consistent and easy to read. The following writing conventions are used:

- Commands are written in *Lucida Console*.
- Pin names are written in **Consolas**.
- File names and User Interface components are written in **bold**.
- Internal cross references are italicized and written in ***semi-bold***.

2 Setting up the Nordic *Bluetooth* Sniffer

Plug PCA10000/PCA10001 into your computer and load it with the Sniffer firmware by performing the following the steps:

1. Connect PCA10000/PCA10001 to a USB port.
2. Place the board between the Peripheral and Central device.

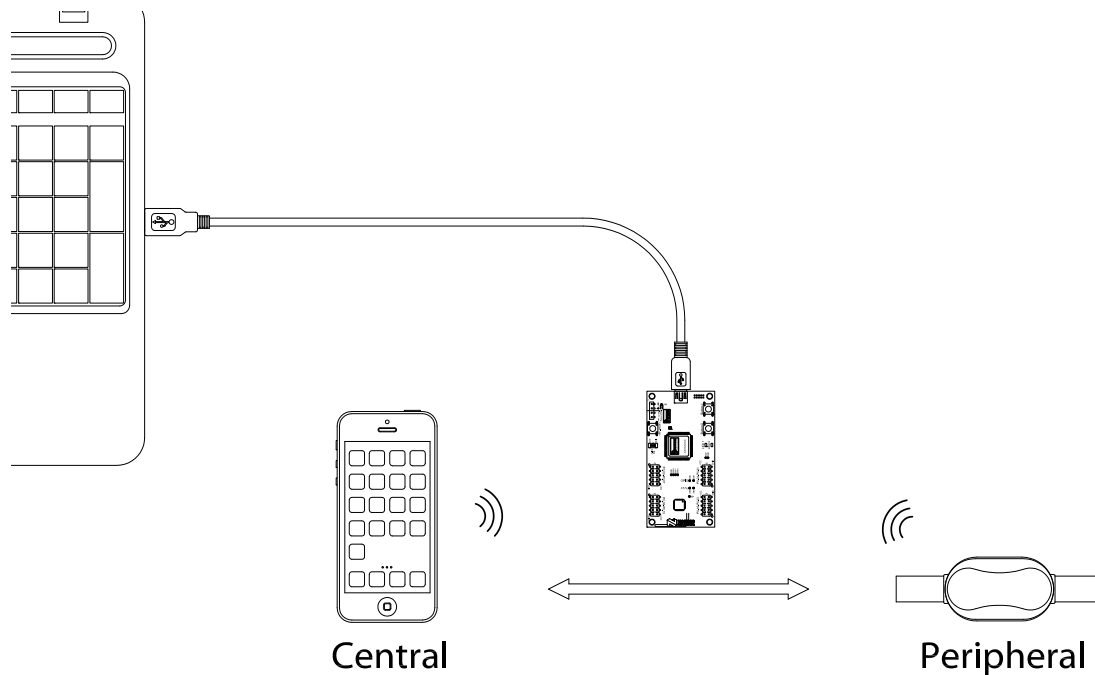


Figure 2 System overview

3. Download and install Wireshark to the default directory.
4. Unzip **ble-sniffer_<os>_<version>_Sniffer.zip**.
5. Open nRFGo Studio.
6. In the Device Manager pane on the left, select the board or dongle to use as a sniffer. It is identified by its SEGGER serial number.
7. Click **Erase all**.
8. Select the **Program Application** tab.
9. Click **Browse** and select **ble-sniffer_nRF51822_<xxx>_sniffer.hex** located in the **Firmware** folder.
10. Click **Program**.
11. If using the Evaluation Kit (PCA10001), **LED1** will toggle each time a packet is received. **LED0** will be lit when the sniffed device is in connection.

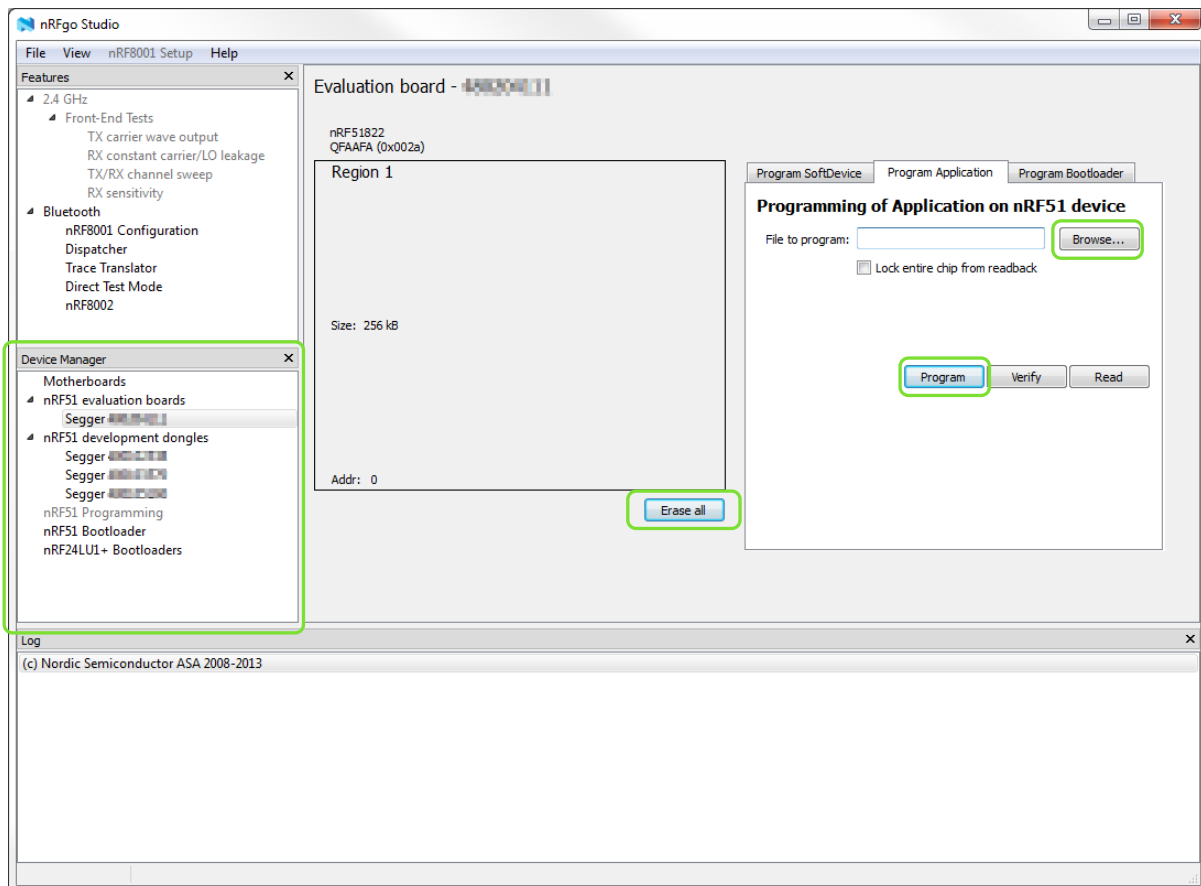


Figure 3 Programming the firmware

2.1 Running the Sniffer

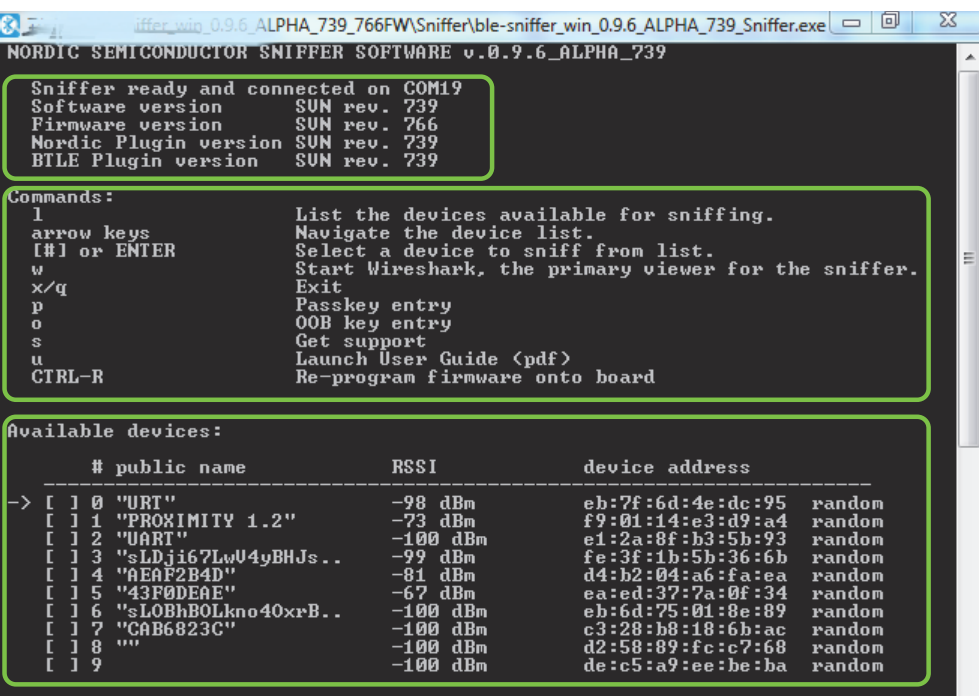
The Sniffer program reports advertisements and lists nearby devices. When starting **ble-sniffer-<os>-<version>.exe** for the first time or installing a new version, use administrator rights. This allows the software to automatically copy plugins to the Wireshark folder tree. For instructions on how to do this manually, see *Chapter 6 "Troubleshooting"* on page 12.

1. Right click **ble-sniffer-<os>-<version>.exe**.
2. Select **Run as administrator**.
3. Provide your password as needed.

Note: Do not remove **ble-sniffer-<os>-<version>.exe** from the sniffer folder. It does not run without the other files.

Once you have the Sniffer program running, the software should automatically find PCA10000/PCA10001 and start reporting advertisements and listing nearby devices. If things aren't working as they should, reset the board and refresh the device list by typing **l** or restart the Sniffer program.

Note: The Sniffer may not manage to pick up all connect requests and will not always pick up on a connection. In such cases, you need to reconnect.



Information

```

NORDIC SEMICONDUCTOR SNIFFER SOFTWARE v.0.9.6_ALPHA_739

Sniffer ready and connected on COM19
Software version      SUN rev. 739
Firmware version     SUN rev. 766
Nordic Plugin version SUN rev. 739
BTLE Plugin version  SUN rev. 739
  
```

Commands

```

Commands:
l          List the devices available for sniffing.
arrow keys Navigate the device list.
[#] or ENTER Select a device to sniff from list.
w          Start Wireshark, the primary viewer for the sniffer.
x/q       Exit
p         Passkey entry
o         OOB key entry
s         Get support
u         Launch User Guide (pdf)
CTRL-R    Re-program firmware onto board
  
```

Device List

```

Available devices:

# public name      RSSI      device address
-----
-> [ 1 0 "URT"      -98 dBm    eb:7f:6d:4e:dc:95 random
[ 1 1 "PROXIMITY 1.2" -73 dBm    f9:01:14:e3:d9:a4 random
[ 1 2 "UART"      -100 dBm   e1:2a:8f:b3:5b:93 random
[ 1 3 "sLDji67LwU4yBHJs.. -99 dBm    fe:3f:1b:5b:36:6b random
[ 1 4 "AEAF2B4D"    -81 dBm    d4:b2:04:a6:fa:ea random
[ 1 5 "43F0DEAE"    -67 dBm    ea:ed:37:7a:0f:34 random
[ 1 6 "sLOBhBOLkno40xrB.. -100 dBm   eb:6d:75:01:8e:89 random
[ 1 7 "CAB6823C"    -100 dBm   c3:28:b8:18:6b:ac random
[ 1 8 ""          -100 dBm   d2:58:89:fc:c7:68 random
[ 1 9 ""          -100 dBm   de:c5:a9:ee:be:ba random
  
```

Figure 4 Sniffer command

3 Using the Sniffer

The Sniffer has two modes of operation:

1. Listens on all advertising channels to try to pick up as many packets as possible from as many devices as possible.
2. Follows one particular device and tries to catch all packets sent to or from this particular device.

The Sniffer always starts in the first mode, showing information for all devices it receives packets from in the Device List, as shown in **Figure 4** on page 6. From this list, you can choose one particular device to sniff, and by that change the mode of the sniffer. As shown in **Table 1** on page 7, this is done by using either the arrow keys and pressing enter or pressing a number from 0-9. You can at any time return to mode 1 by pressing 1.

Keyboard commands

The keyboard commands listed in **Table 1** are used to control the sniffer.

Keyboard command	Description
1	Lists nearby devices. If this command is used while sniffing a device, it will stop sniffing that device. This means if the device is in a connection, the sniffer will lose that connection.
w	Starts Wireshark with the settings necessary to immediately view incoming packets. If Wireshark is started manually, the correct capture interface must be chosen and filters need to be applied manually.
x/q	Exit.
p	You are asked to provide your passkey. Type the 6 digit passkey followed by Enter .
o	You are asked to provide the 16 byte Out-of-band (OOB) key in hexadecimal, big endian format. This must be carried out before the device enters encryption. If the entered key is shorter than 16 bytes, it will be zero-padded in front.
Arrow keys + Enter Numbers 0-9	Selects the device to sniff. While sniffing a device, the device list in the console application will not be updated.
s	Opens online support with detailed help instructions. Here you can report a bug or a problem with the sniffer, or a problem seen on-air with a Nordic Semiconductor device.
u	Launch User Guide in pdf format.
CTRL-r	Re-program Sniffer firmware.

Table 1 Description of controls

4 Using Wireshark

All BLE packets detected by the Sniffer are passed to Wireshark and are wrapped in a header which contains useful meta-information not present in the BLE packet itself. Wireshark dissects the packets and separates the actual packet from the meta-information.

Packet browsing

When a packet is selected in the Packet List, the Details pane shows the dissection of that packet. The bytes of the packet are shown in the Bytes pane. Click a value in Details to highlight it among the bytes, or click on the bytes to highlight it in the Details.

The image shows the Wireshark interface with the following components and annotations:

- Filtering:** The filter bar at the top shows "Filter: btle".
- PACKET LIST:** A table of captured packets. Packet 8350 is selected, showing source 40:34:b0:cf:93:4f and RSSI -77.
- PACKET DETAILS:** The details pane for packet 8350 is expanded, showing:
 - Extra packet information:** Nordic BLE sniffer meta, uart packet counter: 970233, flags: 0x01, encrypted: No, direction: Slave -> Master, CRC: OK, channel: 38, RSSI (dBm): -77, delta time (us end to start): 153, delta time (us start to start): 233.
 - BLE packet:** Bluetooth Low Energy, Access Address: 0x8e89bed6, Packet Header, Init Address: 40:34:b0:cf:93:4f, Advertising Address: f9:01:14:e3:d9:a4, Connection Request, Connection Access Address: 0xaf9a9bde, CRC Init: 0xc75cb2, Window Size (ms): 3.75, Window Offset (ms): 22.5, Interval (ms): 30, Latency: 0, Timeout (ms): 720, Channel map: ffffffff1f, Hop interval: 10, Sleep clock accuracy: 31 ppm to 50 ppm (5), CRC: 0x3f22c1.
- PACKET BYTES:** The bytes pane shows hexadecimal and ASCII representations of the packet data. The first 16 bytes are highlighted in green.
- Wireshark filter for connection interval:** A filter is applied to the packet list: "Interval (ms) (btle.connect.interval), 2 bytes".

Figure 5 Wireshark interface

4.1 Display filtering

Display filters allow you to display a chosen subset of the packets. Most filters are based on the values of the packets, such as length or access address. The filter expressions use Boolean operators (&& || == != !). Some examples are given in *Table 2*.

Display filter	Description
btle.length != 0	Displays only packets where the length field of the BLE packet is not zero, meaning it hides empty data packets.
btle.adv_addr	Displays only packets that have an advertising address, that is, only advertising packets.
(btle.length != 0) && (!btle.adv_addr btle.connect)	A useful filter that will remove all empty data packets, and all advertisement packets except connect requests.
btle	A protocol filter that displays all <i>Bluetooth</i> low energy packets.
btatt, btsmp, btl2cap	Protocol filters for ATT, SMP, and L2CAP packets respectively.

Table 2 Display filtering

4.1.1 Tips

More information can be found on Wireshark's [website](#) by clicking **Get Help** and selecting **Documentation**.

- To get help with constructing filters, click **Expression**.
- Showing a specific part of a packet as a separate column in the packet details can be used to show the connection event of each packet directly in the packet list, or to follow the Sequence Number (SN) and Next Expected Sequence Number (NESN) to check for packet loss. To do this perform the following steps:
 - Select the packet to get the packet details.
 - Right click the part of the packet you want displayed as a column, and click **Apply as Column**.
- You can apply a value as a filter. This can be useful if you want to see only operations affecting a particular handle, for example. To filter packets either having a specific value for some field, do as follows:
 - Right click the value in the packet details, click **Apply as Filter**, and click **Selected**.
- Saving a set of captured packets is useful if they need to be looked at later. To save a set of captured packets do the following:
 - Click the Stop button to quit capturing packets.
 - Click File and select **Save as** to save all packets. Click File and select **Export Specified Packets** to save a selection of packets.
- The Restart button is used to restart a capture and to clear the packet list.
- Each time **Sniffer.exe** is opened, a new capture file and log are started. All captured packets are stored in %APPDATA%\Nordic Semiconductor\Sniffer\logs\capture.pcap.
 - %APPDATA% resolves to C:\Users\[username]\AppData\Roaming.
- Anytime a new filter is applied, the list is automatically scrolled to the packet that is selected.
- You can decide how packets are colored based on display filters. To change this go to **View** and select **Coloring Rules**.

5 Common sniffing actions

Sniffing advertisements from all nearby devices

To see advertisements from all nearby devices:

1. Start the Sniffer.
2. Press w to run Wireshark.

Sniffing advertisement packets involving a single slave device

To see advertisement packets, scan requests, and scan responses to and from a single device:

1. Start the Sniffer if not already running.
2. Press w to run Wireshark if it's not already running.
3. In the Sniffer program, choose the device from the device list.

Sniffing a connection involving a single slave device

To sniff a connection between a specific Peripheral device and a Central:

1. Start the Sniffer if not already running.
2. Press w to run Wireshark if it's not already running.
3. In the Sniffer program, choose the device from the device list.
4. Connect the Central to the Peripheral.

Just Works - sniffing an encrypted connection

To sniff a connection encrypted with Just Works:

1. Start the Sniffer if not already running.
2. Press w to run Wireshark if it's not already running.
3. In the Sniffer program, choose the device from the device list.
4. Initiate pairing between the devices if it does not happen automatically. The Sniffer will automatically decrypt encrypted packets.

To sniff a connection between devices that are already paired, the Sniffer needs to have sniffed the pairing procedure. If the sniffer board is reset, stored pairing information will be lost.

Passkey - sniffing an encrypted connection

To sniff a connection encrypted with passkey:

1. Start the Sniffer if not already running.
2. Press w to run Wireshark if it's not already running.
3. In the Sniffer program, choose the device from the device list.
4. Initiate pairing between the devices if it does not happen automatically. A passkey will be displayed on either the Central or the Peripheral.
5. Enter the passkey into the Sniffer command by pressing p and typing the passkey digits as they are displayed.
6. Press **Enter**.
7. Enter the passkey into the other device after having entered it into the Sniffer command.

OOB - sniffing an encrypted connection

To sniff a connection encrypted with OOB:

1. Start the Sniffer if not already running.
2. Press **w** to run Wireshark if it's not already running.
3. In the Sniffer program, choose the device from the device list.
4. Enter the OOB key into the Sniffer command before the devices initiate pairing.
 - Press **o**.
 - Type the OOB key in big-endian, hexadecimal format. Leading zero-bytes may be omitted.
 - Press **Enter**.
5. Connect the Central to the Peripheral.
6. Initiate pairing between the devices if it does not happen automatically.

6 Troubleshooting

The Sniffer is connected to the computer and it says “Finding Sniffer Dongle” but it is taking a while to find the dongle.

1. Make sure no other program is using the Sniffer serial port, including other instances of the Sniffer software.
2. Unplug the board and wait 10 seconds.
3. Plug it back in.

If it still can't find the Sniffer dongle you might have to specify the Sniffer's COM port number.

1. To find the COM port number in the Windows Device Manager, click **Start**, select **Run**, and then type **devmgmt.msc**.
2. The COM port number is located in the **Ports (COM & LPT)** menu.
3. Open the Sniffer folder and then open **sniffer.cfg** in a text editor like Notepad.
4. Set the comPort property to the COM port number used for the dongle. For example, **comPort=54** if the dongle is on COM54.

Wireshark does not recognize btle or nordic_ble, and the Sniffer program cannot find version information for the plugins.

Run the Sniffer as Administrator. This should install the plugin automatically.

If you are running the Sniffer program manually:

1. Copy **btle.dll** and **nordic_ble.dll** from the Sniffer directory to **<Wireshark installation>\plugins\<version>**.
2. Use the files in **...\plugins** if your Wireshark version is 64 bit, or the files in **...\plugins\win32** if Wireshark is 32 bit.

Opening Wireshark with the w command does not work. How can I open Wireshark manually?

1. Run the Sniffer.
2. Open Wireshark.
3. Click **Interface List**, then click **Options, Manage Interfaces**, and select **New**.
4. In the **Pipe** field type **\\.\pipe\wireshark_nordic_ble**. Click **Save** and close the configuration windows.
5. Apply the filter **btle** and click **Start**.

Packets are not being picked up by the sniffer.

The Sniffer board should be placed between the Central and Peripheral.

Wireshark is not able to display the sniffed packets.

The Sniffer will generate a Wireshark capture file (**%APPDATA%\Nordic Semiconductor\capture.pcap**) which can be viewed afterwards even if real time viewing is not used. Press **S** to view the folder with the file.

The Sniffer starts showing “Malformed packets” after a while when sniffing an encrypted link.

This is a known limitation with the Sniffer, which will be improved in future releases. See the release notes for details.

Liability disclaimer

Nordic Semiconductor ASA reserves the right to make changes without further notice to the product to improve reliability, function or design. Nordic Semiconductor ASA does not assume any liability arising out of the application or use of any product or circuits described herein.

Life support applications

Nordic Semiconductor's products are not designed for use in life support appliances, devices, or systems where malfunction of these products can reasonably be expected to result in personal injury. Nordic Semiconductor ASA customers using or selling these products for use in such applications do so at their own risk and agree to fully indemnify Nordic Semiconductor ASA for any damages resulting from such improper use or sale.

Contact details

For your nearest distributor, please visit <http://www.nordicsemi.com>.

Information regarding product updates, downloads, and technical support can be accessed through your My Page account on our homepage.

Main office: Otto Nielsens veg 12
 7052 Trondheim
 Norway
 Phone: +47 72 89 89 00
 Fax: +47 72 89 89 89

Mailing address: Nordic Semiconductor
 P.O. Box 2336
 7004 Trondheim
 Norway



Revision History

Date	Version	Description
April 2014	1.1	Updated firmware, now supports all versions of PCA10000 and PCA10001.
December 2013	1.0	First release.