ANR004 PROTEUS

HOW TO USE THE PERIPHERAL ONLY MODE

VERSION 2.4

FEBRUARY 16, 2021

Revision history

Manual version	Notes	Date
1.0	• Initial version	February 2017
1.1	• Updated MTU size to 247 bytes	July 2017
2.0	• New corporate design	June 2018
2.1	• Updated product name from AMB2621 to Proteus-I	November 2018
2.2	• Updated file name to new AppNote name structure. Updated important notes, legal notice & license terms chapters.	June 2019
2.3	• Added Proteus-II and Proteus-III description • Updated address of Division Wireless Connectivity & Sensors location	January 2020
2.4	• Restructured app note • Added new chapter `Quickstart` with new connection setup examples • Added information on the Proteus-III mini evaluation board	February 2021

Abbreviations and abstract

Abbreviation	Name	Description
BTMAC		Bluetooth® conform MAC address of the module used on the RF-interface.
CS	Checksum	Byte wise XOR combination of the preceding fields.
DTM	Direct test mode	Mode to test Bluetooth® specific RF settings.
GAP	Generic Access Profile	The GAP provides a basic level of functionality that all Bluetooth® devices must implement.
I/O	Input/output	Pinout description.
LPM	Low power mode	Mode for efficient power consumption.
LSB	Least significant bit	
MAC		MAC address of the module.
MSB	Most significant bit	
MTU	Maximum transmission unit	Maximum packet size of the Bluetooth® connection.
Payload		The intended message in a frame / package.
RF	Radio frequency	Describes wireless transmission.
RSSI	Receive Signal Strength Indicator	The RSSI indicates the strength of the RF signal. Its value is always printed in two's complement notation.
Soft device		Operating system used by the nRF52 chip.
UART	Universal Asynchronous Receiver Transmitter	Allows the serial communication with the module.
[HEX] 0xhh	Hexadecimal	All numbers beginning with 0x are hexadecimal numbers. All other numbers are decimal, unless stated otherwise.

Contents

1 Introduction

The Proteus is a Bluetooth® module based on the nRF52 Nordic Semiconductors SoC which provides various Bluetooth® LE and low power features.
In addition to the standard command mode, that uses predefined commands to run and configure the radio module, Würth Elektronik eiSos launches the "peripheral only mode" on the Proteus to use the module as Bluetooth® LE bridge in a simple way.
In this mode, a Bluetooth® LE interface using the static passkey authentication method (with bonding) and a transparent UART interface is provided, such that no configuration of the module is required to equip a custom application with it.
In case the user needs a non-standard configuration, it can be configured in advance using the command mode, or upon request Würth Elektronik eiSos can apply customer specific configurations during the production process.
The following chapters describe how to set the module into peripheral only mode and which steps have to be applied to establish a connection to the radio module.

2 Prerequisites

- A Proteus evaluation board in factory state, for example
  - the Proteus-I evaluation board with firmware version 3.0.0 or newer.
  - the Proteus-II evaluation board.
  - the Proteus-III evaluation board or mini evaluation board.
- A central device, that initiates the connetion setup. For example
  - a smart phone with Bluetooth® LE function and the Nordic Semiconductor nRF Connect App.
  - another Proteus evaluation board or mini evaluation board.
  - a Proteus Plug (radio stick containing a Proteus radio module).

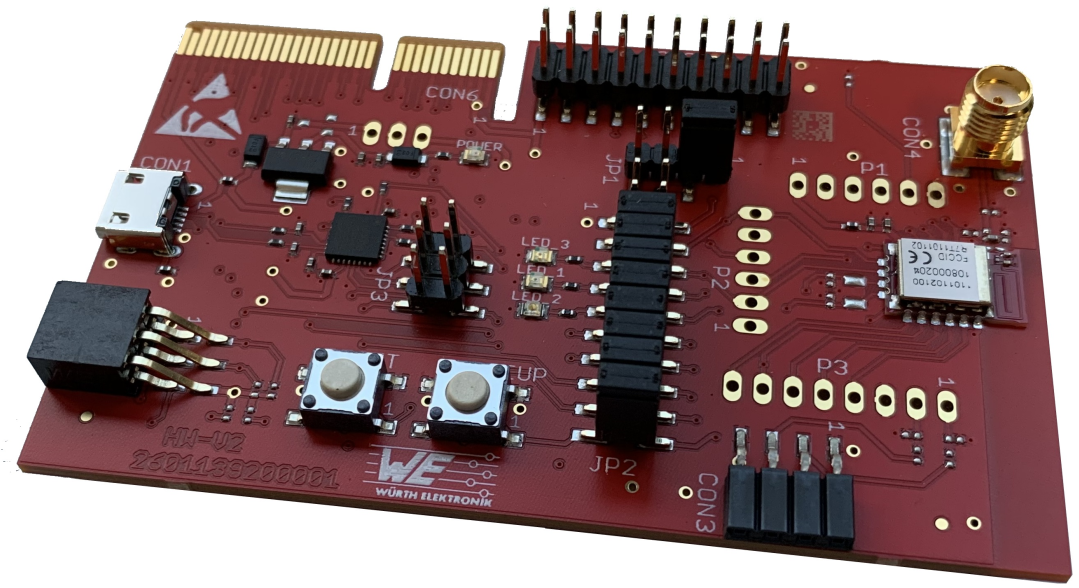


Figure 1: Proteus-III evaluation board

To be sure that the Proteus radio module or Proteus Plug is in factory state, please run a factory reset before doing any other action.

Please check whether the most recent firmware is installed on any Proteus radio module, EV board or Proteus Plug.

3 Peripheral only mode: General information

For a better understanding of the content of this chapter, basic knowledge of the Bluetooth® standard as well as that of the SPP-like profile is of advantage. Please find more details on that in the respective advanced developer guide:

- ANR002 Proteus-I advanced developer guide
- ANR005 Proteus-II advanced developer guide
- ANR009 Proteus-III advanced developer guide

3.1 How to set the Proteus radio module to peripheral only mode?

The Proteus starts in peripheral only mode, when a HIGH level is applied at the *OPERATION_MODE* pin and a reset is done via the */RESET* pin. If the *OPERATION_MODE* pin is LOW during the reset, the module starts in normal operation mode with command interface.

> ! A pull-down is applied to the *OPERATION_MODE* pin during start-up. Thus increased currents can occur for a period $\leq$ 1 ms.

> ! After the start-up procedure has been finished, the *OPERATION_MODE* pin and thus the applied signal level has no function.

> ! For Proteus-III, the *OPERATION_MODE* pin has been renamed to *MODE_1*, while maintaining the same function. Throughout this app note we will use *OPERATION_MODE* as a term for this pin.

In case of the evaluation board for Proteus, simply connect the *OPERATION_MODE* pin to *VCC* by setting the respective jumper (see figure 2, 3 and 4). Then press the reset button to start the module in peripheral only mode.

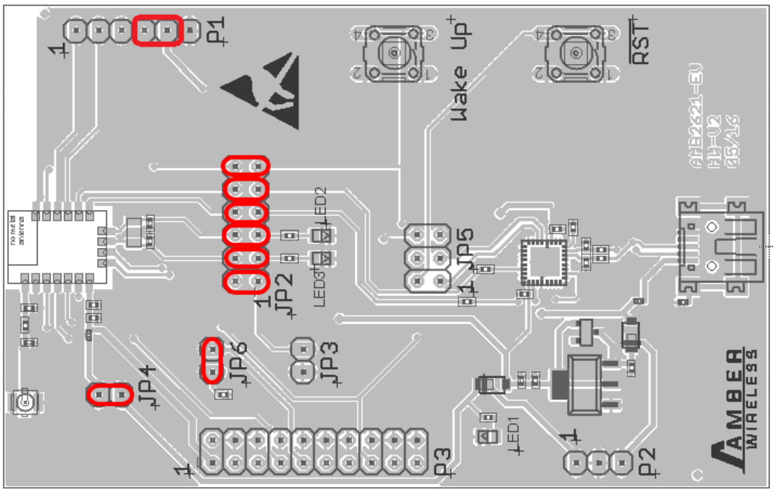


Figure 2: On Proteus-I and Proteus-II evaluation board, set these jumpers to start the peripheral only mode after reset.

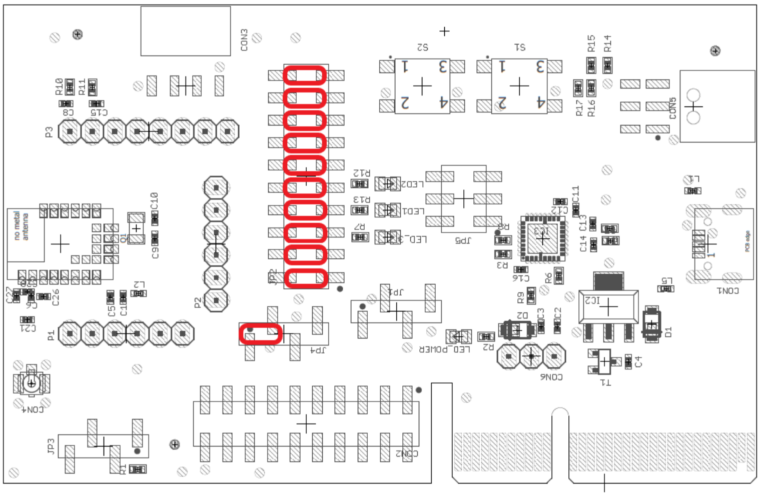


Figure 3: On Proteus-III evaluation board, set these jumpers to start the peripheral only mode after reset.

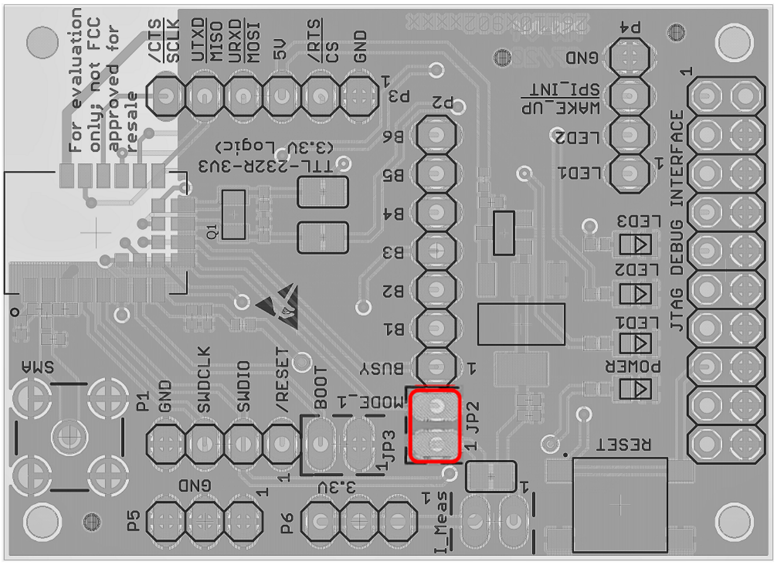


Figure 4: On Proteus-III mini evaluation board, set these jumpers to start the peripheral only mode after reset.

3.2 General connection setup information

In factory state, the peripheral only mode uses the static passkey pairing with bonding authentication method, which requests a static passkey from the connecting device. Figure 5 shows the steps that have to be performed successively during connection setup using the static passkey pairing method:

1. Physical connection establishment
   A physical connection has to be established first. Therefore, a central device (usually smart phone) has to connect to the Proteus which runs as peripheral.

2. Pairing process
   The authentication and exchange of encryption information is part of the pairing process. The central device must request at least the same security level to access the characteristics of the Proteus. The peripheral only mode uses static passkey bonding by default. The Proteus waits for the bonding request of the central device to perform this step.

> STOP
>
> In case the central device goes on with the next steps without placing this bonding request, the peripheral device disconnects immediately as the required security level is not achieved. The same holds, if the central device places a bonding request with lower security level than required by the peripheral device (static passkey with bonding).

3. Exchange of the maximum transmission unit (MTU)
   The maximum transmission unit can be increased to allow the transmission of larger data packets. The Proteus allows an MTU of up to 247 bytes, which results in a payload of up to 243 bytes. This step is optional. Not selecting a higher MTU will use the Bluetooth® LE 4.0 default MTU which results in 19 bytes payload for the user but will be compatible to pre Bluetooth® LE 4.2 devices.

4. Discover the characteristics of the Proteus SPP-like profile
   The characteristics offered by the Proteus have to be discovered by the central.

5. Notification enable
   The peripheral must let the central know, when there is new data. Therefore, notifications have to be enabled. After this step, the channel is open and data transmission can start.

For the description, we assume that a smart phone is the initiator of the connection. Thus, it acts as central and the Proteus acts as peripheral in figure 5.

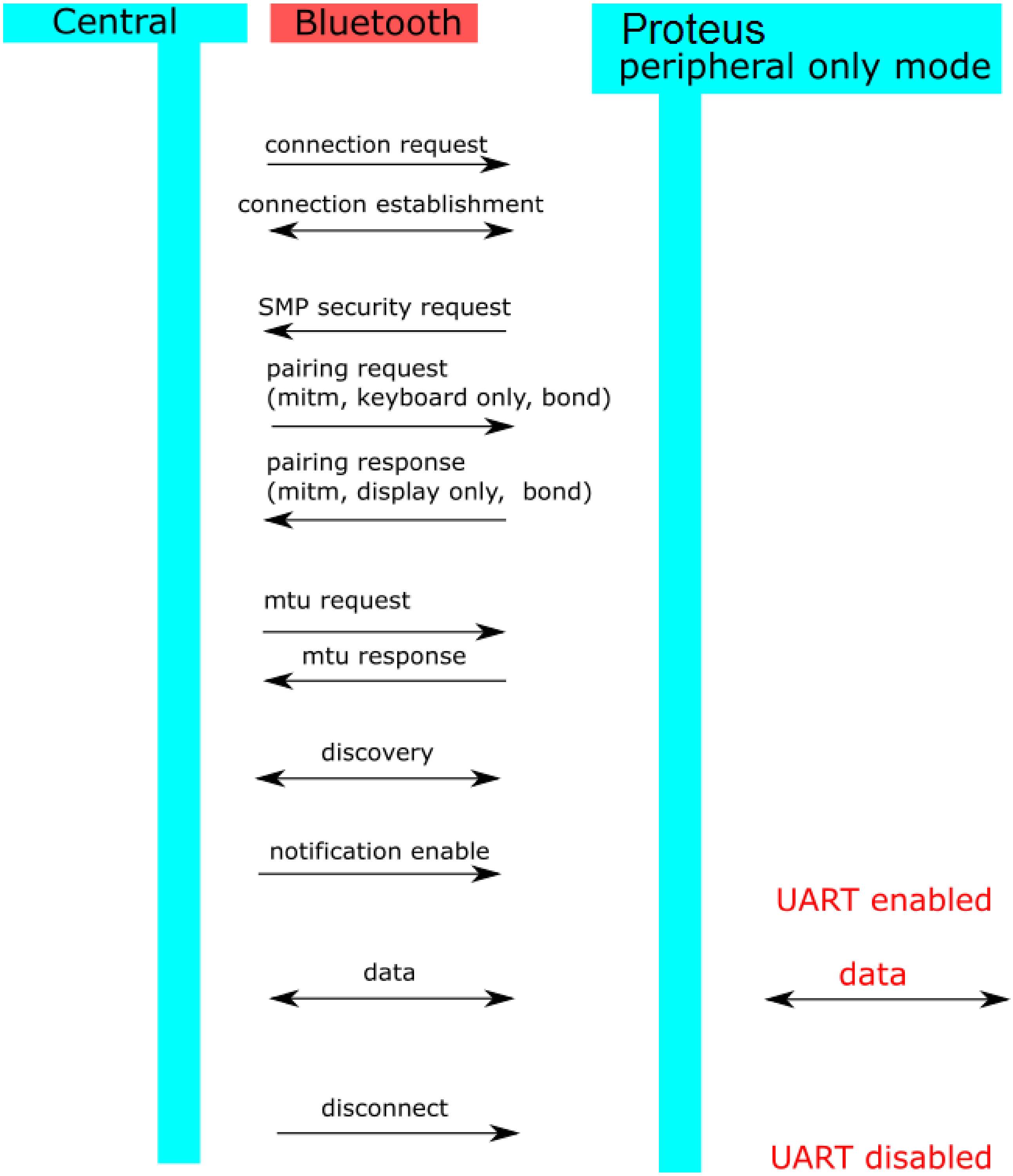


Figure 5: Steps for the connection setup in static passkey mode (default)

3.3 Preconfiguring of the module

In case user settings (such as UART baud rate, security mode or the static passkey value) have to be modified, please start the module in normal mode (apply a low signal at the *OPERATION MODE* pin during start-up). Then use the commands like `CMD_SET_REQ` to update these user settings and switch back to peripheral only mode (apply a high signal to the *OPERATION MODE* pin during start-up).

STOP For security reasons it is strongly recommended to change the default `RF_StaticPasskey` to a customer specific passkey.

! Custom product: Upon request Würth Elektronik eiSos can apply customer specific configuration(s) during the production process.

4 Quickstart

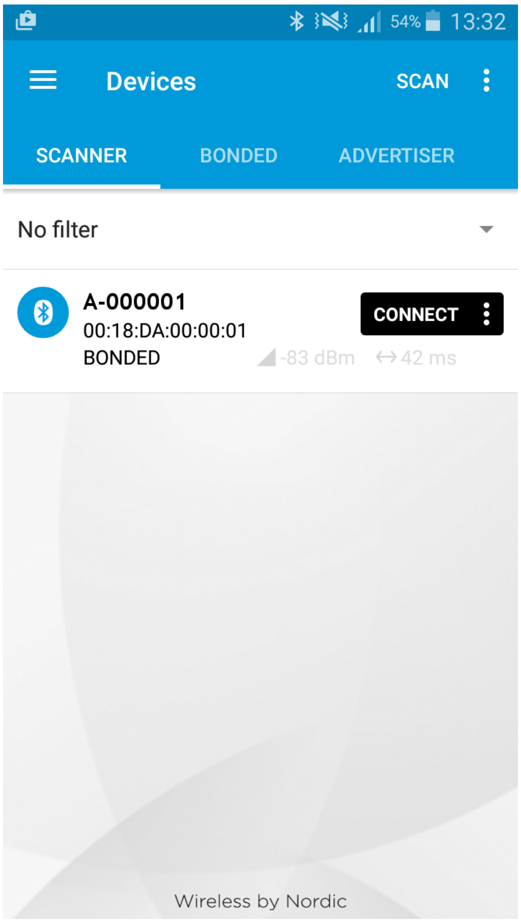
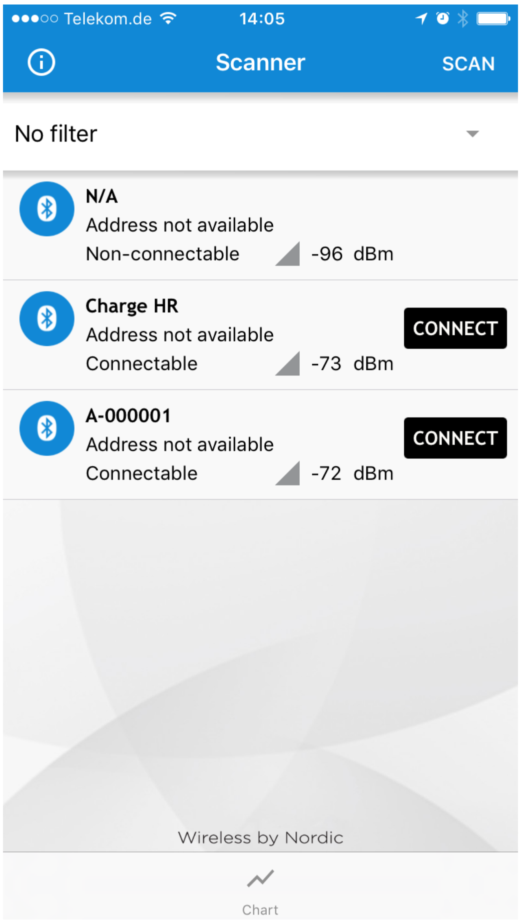
In chapter 3.2, it has been described which steps have to be performed by the central device to setup a connection to a Proteus radio module running in peripheral only mode. What this means in practice will be shown in this chapter. Two examples are following. First, how to use a smart phone and the nRF Connect App to setup a connection to a Proteus radio module running in peripheral only mode (see chapter 4.1). And second, how to use another Proteus radio module or Proteus plug to do so (see chapter 4.3).

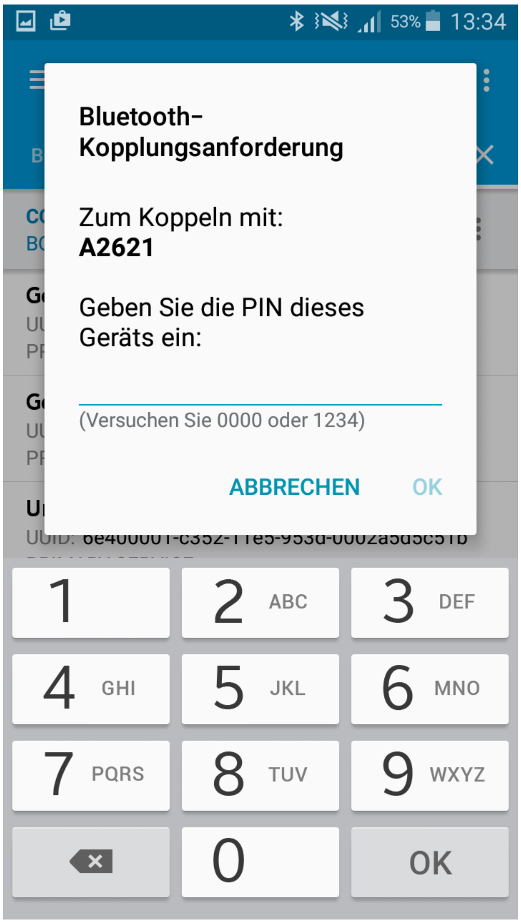
4.1 Smart phone using nRFConnect app as central device

This chapter describes how to setup a connection to the Proteus radio module in peripheral mode (factory state), when a smart phone and the nRF Connect App are used.

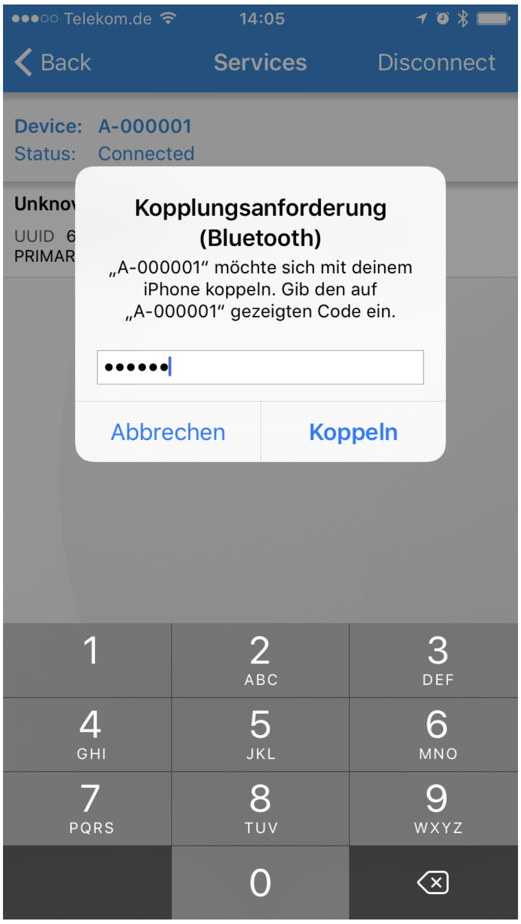
> ❗ The nRF Connect App is an open source App providing standard Bluetooth® LE functions for iOS as well as for Android devices.

Please perform the following steps:

<table>
<tr><th>Android</th><th>iOS</th></tr>
<tr><td colspan="2">
<ul>
<li>Connect the module to a PC and open a terminal program using the Proteus default UART settings (115200 Baud, 8n1).</li>
<li>Set the module into peripheral only mode as described in chapter <code>3.1</code>. Initially, the module is advertising. Thus the Proteus <i>LED_1</i> is blinking.</li>
<li>Start your smart phone, enable the Bluetooth® LE feature and start the nRF Connect App.</li>
<li>Press "SCAN" to find the module on the radio.</li>
<li>When the module A-xxxxxx appears, press connect. (Note: the part after "A-" is the 3 LSB as ASCII hex of the BTMAC, the fixed part "0x0018DA" is not part of the device descriptor).</li>
</ul>
</td></tr>
<tr><td>

54% 13:32
Devices SCAN
SCANNER BONDED ADVERTISER
No filter
A-000001
00:18:DA:00:00:01
BONDED -83 dBm ↔42 ms
CONNECT
Wireless by Nordic
</td><td>

●●●○○ Telekom.de 14:05
Scanner SCAN
No filter
N/A
Address not available
Non-connectable -96 dBm
Charge HR
Address not available
Connectable -73 dBm
CONNECT
A-000001
Address not available
Connectable -72 dBm
CONNECT
Wireless by Nordic
Chart
</td></tr>
</table>

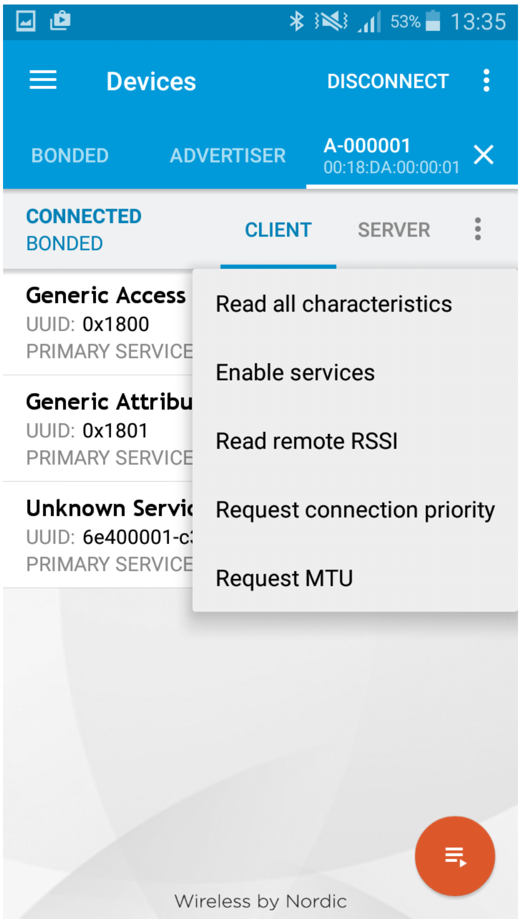
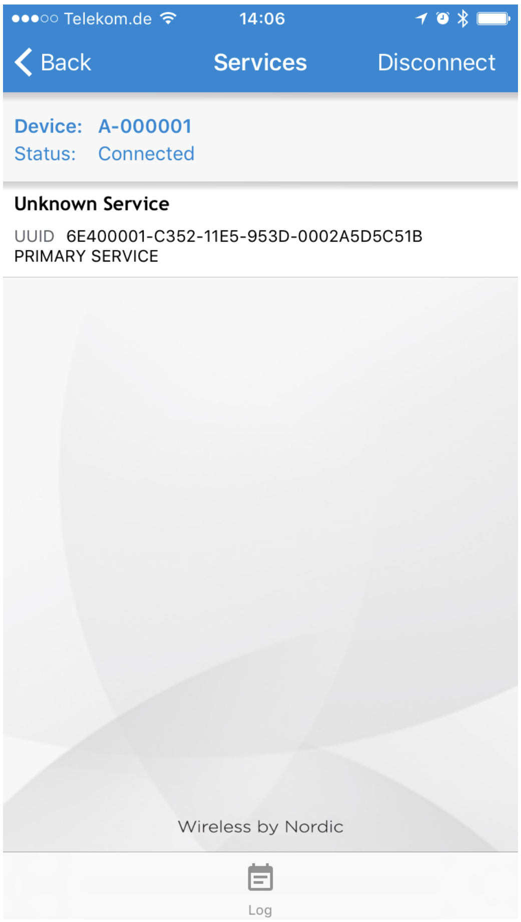
<table>
<tr><th>Android</th><th>iOS</th></tr>
<tr><td colspan="2">• As soon as the module has received the connection request the module <i>LED_1</i> (<i>LED_3</i> on the Proteus-EV) will constantly light up.
• Then the radio module requests for the static passkey. In default, the passkey is "123123".
• The Bluetooth® coupling requirement popup is shown in your smartphone.
• When the bonding feature is enabled in the authentication settings and the bonding information already exists, a re-entering of the passkey is not required when reconnecting.</td></tr>
<tr><td>
Bluetooth-Kopplungsanforderung
Zum Koppeln mit: **A2621**
Geben Sie die PIN dieses Geräts ein:
(Versuchen Sie 0000 oder 1234)
ABBRECHEN OK

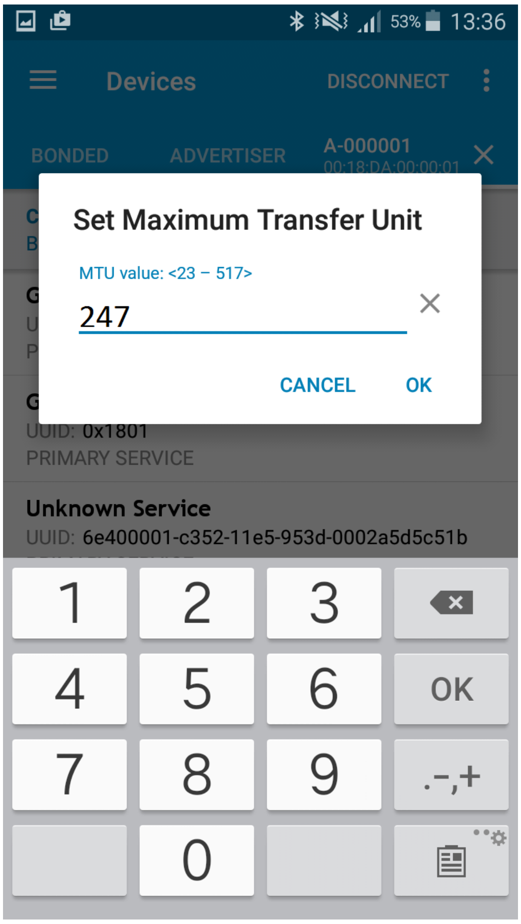
53% 13:34
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0
OK

</td>
<td>
Device: A-000001
Status: Connected
Kopplungsanforderung (Bluetooth)
„A-000001“ möchte sich mit deinem iPhone koppeln. Gib den auf „A-000001“ gezeigten Code ein.
••••••
Abbrechen Koppeln

Telekom.de 14:05
Back
Services
Disconnect
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0

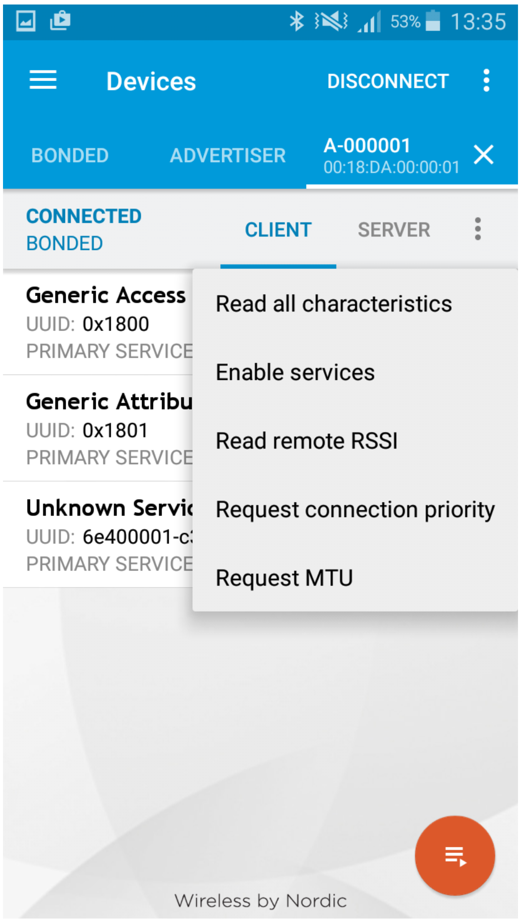
</td></tr>
</table>

Android	iOS
• Now you are authenticated. • Please click on the menu bullets on the right and press "Request MTU" to request for a larger MTU. 	• Now you are authenticated. • Please click on the "Unknown Service" to start the service discovery and the MTU request. 

Android	iOS
• The Proteus allows an MTU of up to 247 bytes, which results in a payload size of 243 bytes.  Set Maximum Transfer Unit MTU value: <23 – 517> 247 13:36 53% Devices DISCONNECT BONDED ADVERTISER A-000001 00:18:DA:00:00:01 CANCEL OK UUID: 0x1801 PRIMARY SERVICE Unknown Service UUID: 6e400001-c352-11e5-953d-0002a5d5c51b	• The iOS App runs this step simultaneously in the background, a user-defined MTU is not possible.

<table>
<tr><th>Android</th><th>iOS</th></tr>
<tr><td>

- Again click on the menu bullets on the right and press "Enable services" to enable the notifications.



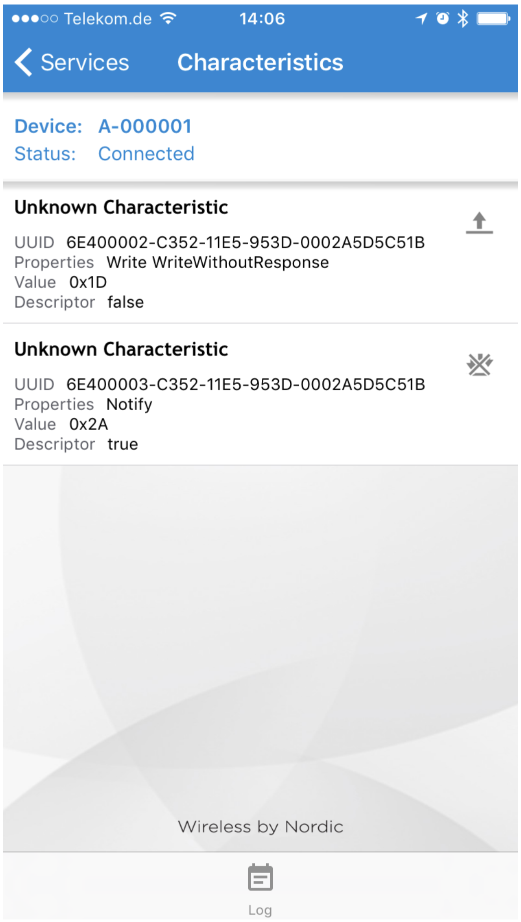
Generic Access
UUID: 0x1800
PRIMARY SERVICE

Generic Attribu
UUID: 0x1801
PRIMARY SERVICE

Unknown Servic
UUID: 6e400001-c:
PRIMARY SERVICE

</td><td>

- Press the arrows on the RX-characteristic `6E400003- C352- 11E5- 953D -0002A5D5C51B` to enable the notifications. Press it until a cross appears (see below, it has to be pressed at least once). If a cross is already shown press it twice so the cross disappears and then reappears.



Device: A-000001
Status: Connected

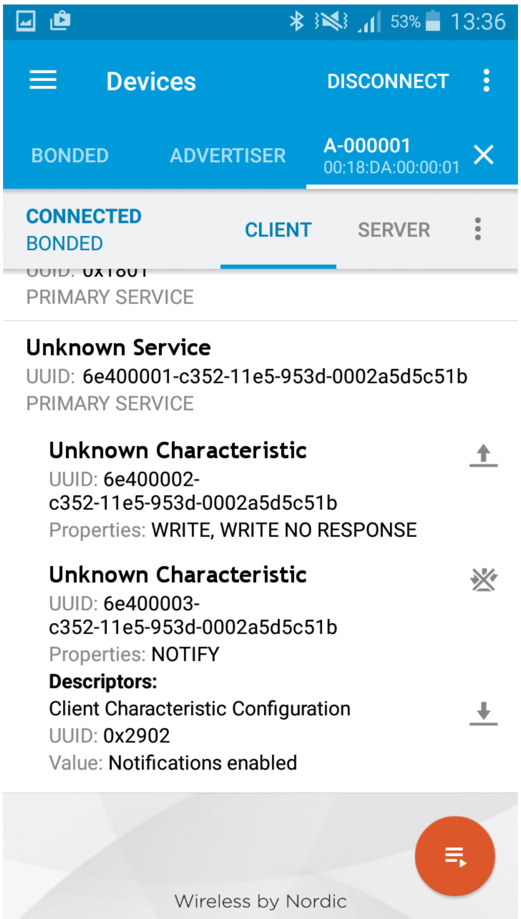
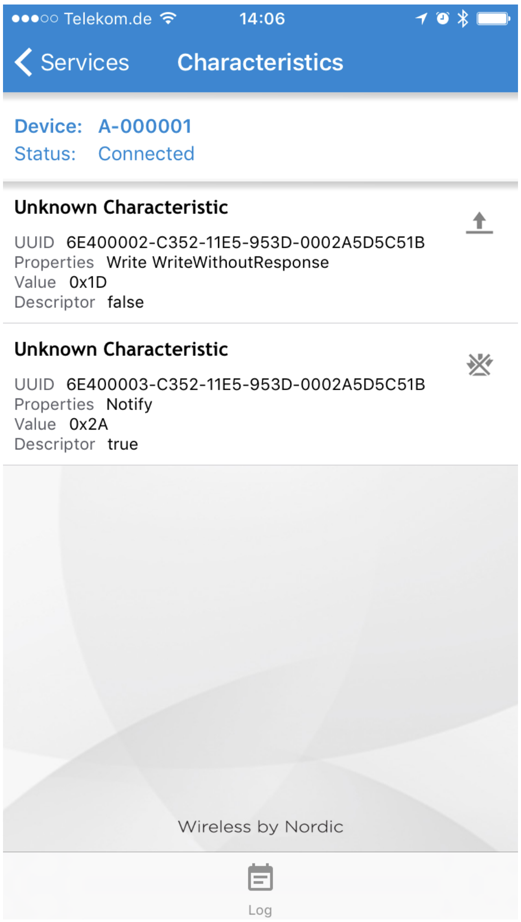
Unknown Characteristic
UUID 6E400002-C352-11E5-953D-0002A5D5C51B
Properties Write WriteWithoutResponse
Value 0x1D
Descriptor false

Unknown Characteristic
UUID 6E400003-C352-11E5-953D-0002A5D5C51B
Properties Notify
Value 0x2A
Descriptor true

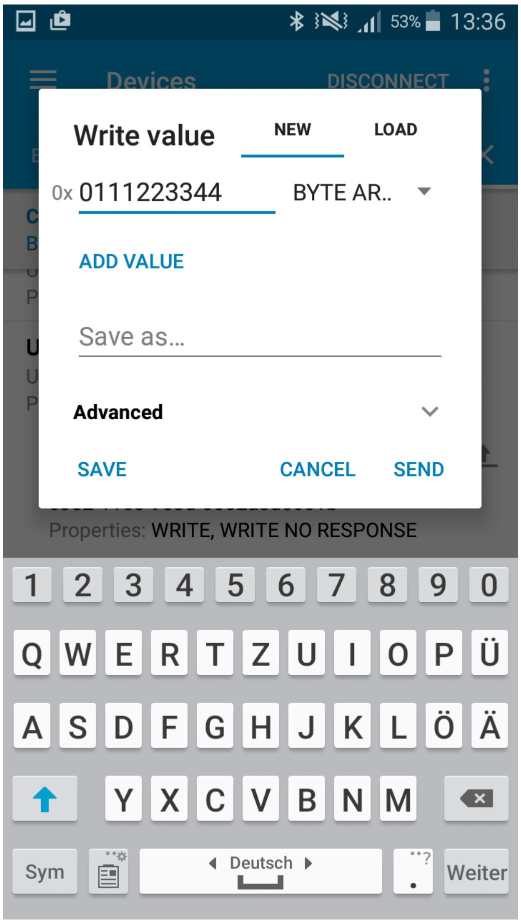
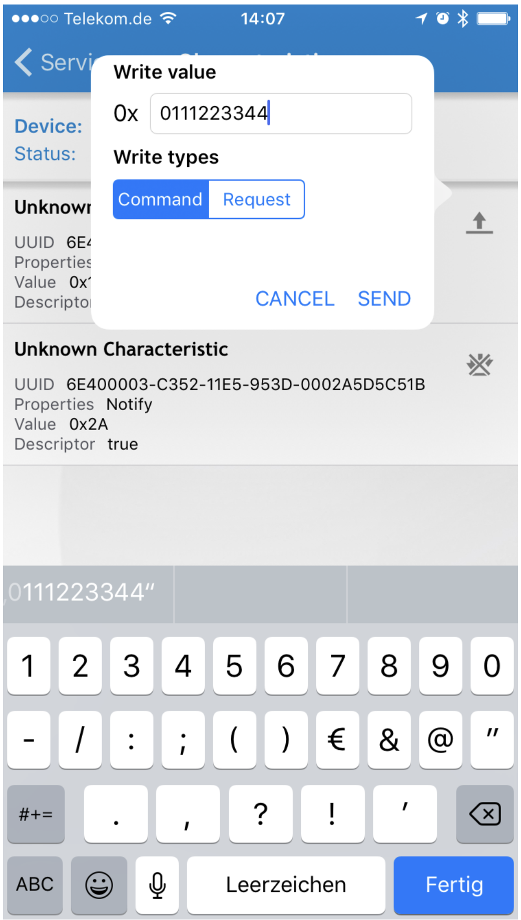
</td></tr>
<tr><td colspan="2">

- As soon as the module has received the notification enable request the Proteus *LED_2* (*LED_2* on the Proteus-EV) is turned on.

</td></tr>
</table>

Android	iOS
 53% 13:36 Devices DISCONNECT BONDED ADVERTISER A-000001 00:18:DA:00:00:01 CONNECTED BONDED CLIENT SERVER UUID: 0x1801 PRIMARY SERVICE Unknown Service UUID: 6e400001-c352-11e5-953d-0002a5d5c51b PRIMARY SERVICE Unknown Characteristic UUID: 6e400002-c352-11e5-953d-0002a5d5c51b Properties: WRITE, WRITE NO RESPONSE Unknown Characteristic UUID: 6e400003-c352-11e5-953d-0002a5d5c51b Properties: NOTIFY **Descriptors:** Client Characteristic Configuration UUID: 0x2902 Value: Notifications enabled Wireless by Nordic	 ●●●○○ Telekom.de 14:06 Services Characteristics Device: A-000001 Status: Connected Unknown Characteristic UUID 6E400002-C352-11E5-953D-0002A5D5C51B Properties Write WriteWithoutResponse Value 0x1D Descriptor false Unknown Characteristic UUID 6E400003-C352-11E5-953D-0002A5D5C51B Properties Notify Value 0x2A Descriptor true Wireless by Nordic Log

- Now you are fully connected and you can access the characteristics. The maximum size of payload depends on the chosen MTU size. Here we chose 247 bytes, which allows us to send 243 bytes of payload via the channel.
- To send data to the Proteus, press the arrow next to the TX-characteristic `6E400002-C352-11E5-953D-0002A5D5C51B`.
- Then enter 0x01 as header byte followed by your payload (for example 0x11 0x22 0x33 0x44) and press "SEND". The payload size is dependent on the MTU that was negotiated in the connection process. The smallest supported MTU for all Bluetooth® 4.0 (or newer) devices results in a max payload (after the 0x01 header) of 19 bytes.

Android	iOS
	

Write value

0x 0111223344 BYTE AR..

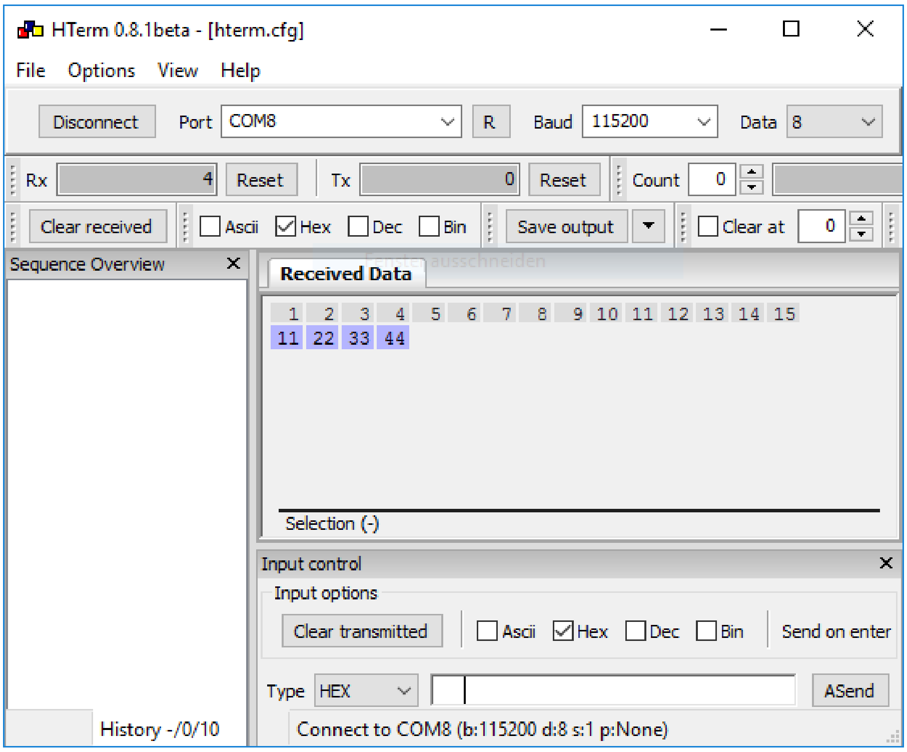
Write value

0x 0111223344

Write types: Command | Request

- The payload that has been sent via radio is output by the Proteus via UART. In peripheral only mode, a transparent UART interface is used. This means, that only payload data is transmitted, without any packet header or footer. Thus the transmitted bytes 0x11 0x22 0x33 0x44 are displayed on the connected terminal program.

Android	iOS



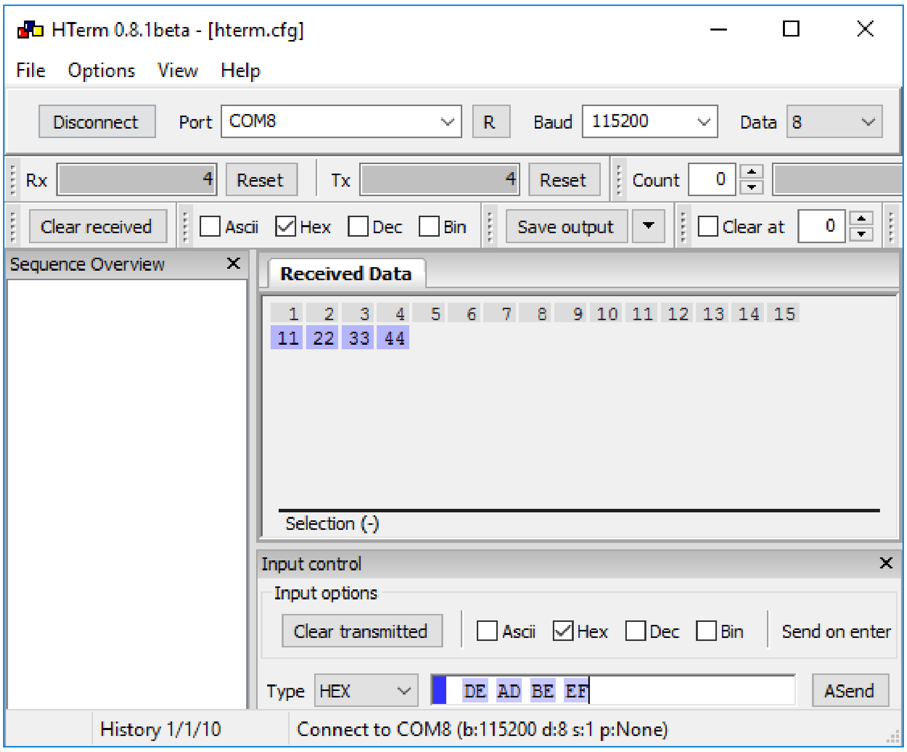
Port COM8 Baud 115200 Data 8
Rx 4 Tx 0 Count 0
☐ Ascii ☑ Hex ☐ Dec ☐ Bin ☐ Clear at 0

```
 1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
11 22 33 44
```

Selection (-)

☐ Ascii ☑ Hex ☐ Dec ☐ Bin
Type HEX
History -/0/10
Connect to COM8 (b:115200 d:8 s:1 p:None)

- To send back data simply enter your payload in the respective terminal program field and press enter. In this example we choose 0xDE 0xAD 0xBE 0xEF. The header 0x01 will be automatically applied by the module and is not to be transmitted by the host.
- Here again the maximum payload size (MTU) must be respected.



Port COM8 Baud 115200 Data 8
Rx 4 Tx 4 Count 0
☐ Ascii ☑ Hex ☐ Dec ☐ Bin ☐ Clear at 0

```
 1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
11 22 33 44
```

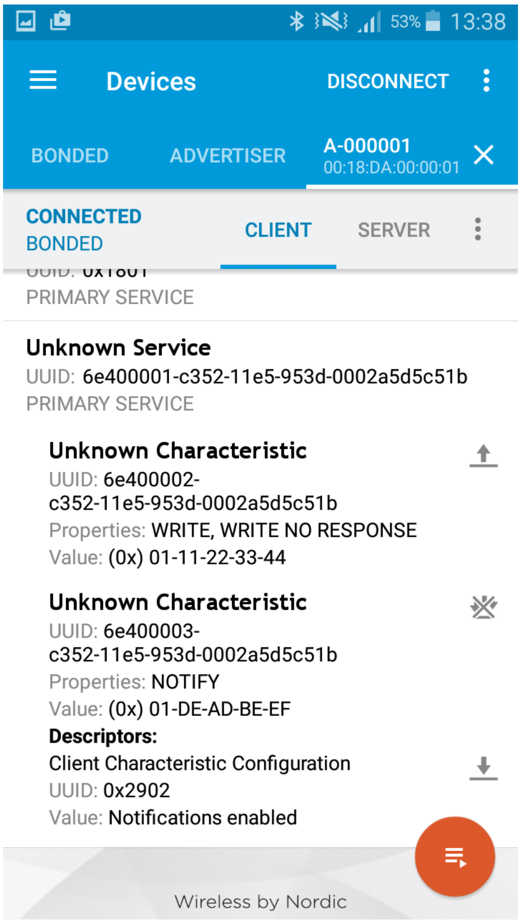
Selection (-)

☐ Ascii ☑ Hex ☐ Dec ☐ Bin
Type HEX DE AD BE EF
History 1/1/10
Connect to COM8 (b:115200 d:8 s:1 p:None)

<table>
<tr><th>Android</th><th>iOS</th></tr>
<tr><td colspan="2">

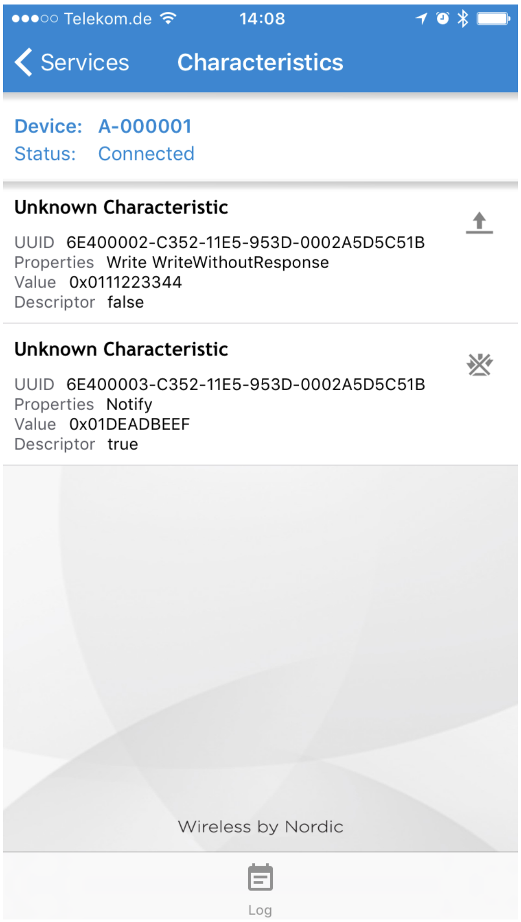
- The received data can be found in the RX-characteristic `6E400003-C352-11E5-953D-0002A5D5C51B`. It contains the header byte 0x01 and the payload 0xDE 0xAD 0xBE 0xEF.

</td></tr>
<tr><td>



53% 13:38
Devices DISCONNECT
BONDED ADVERTISER A-000001 00:18:DA:00:00:01
CONNECTED
BONDED
CLIENT SERVER
UUID: 0x1801
PRIMARY SERVICE
Unknown Service
UUID: 6e400001-c352-11e5-953d-0002a5d5c51b
PRIMARY SERVICE
Unknown Characteristic
UUID: 6e400002-c352-11e5-953d-0002a5d5c51b
Properties: WRITE, WRITE NO RESPONSE
Value: (0x) 01-11-22-33-44
Unknown Characteristic
UUID: 6e400003-c352-11e5-953d-0002a5d5c51b
Properties: NOTIFY
Value: (0x) 01-DE-AD-BE-EF
Descriptors:
Client Characteristic Configuration
UUID: 0x2902
Value: Notifications enabled
Wireless by Nordic

</td><td>



●●●○○ Telekom.de 14:08
< Services Characteristics
Device: A-000001
Status: Connected
Unknown Characteristic
UUID 6E400002-C352-11E5-953D-0002A5D5C51B
Properties Write WriteWithoutResponse
Value 0x0111223344
Descriptor false
Unknown Characteristic
UUID 6E400003-C352-11E5-953D-0002A5D5C51B
Properties Notify
Value 0x01DEADBEEF
Descriptor true
Wireless by Nordic
Log

</td></tr>
</table>

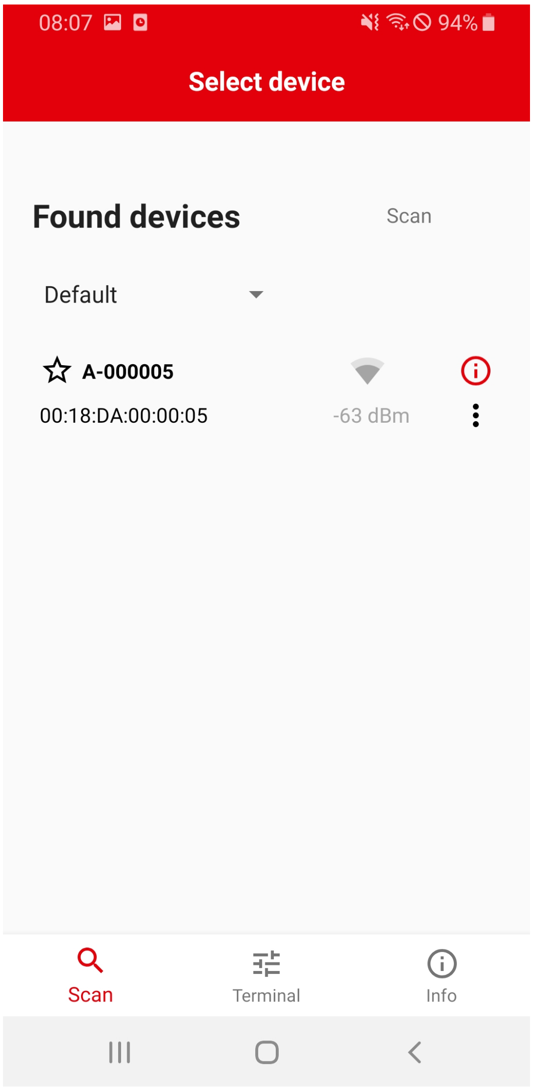
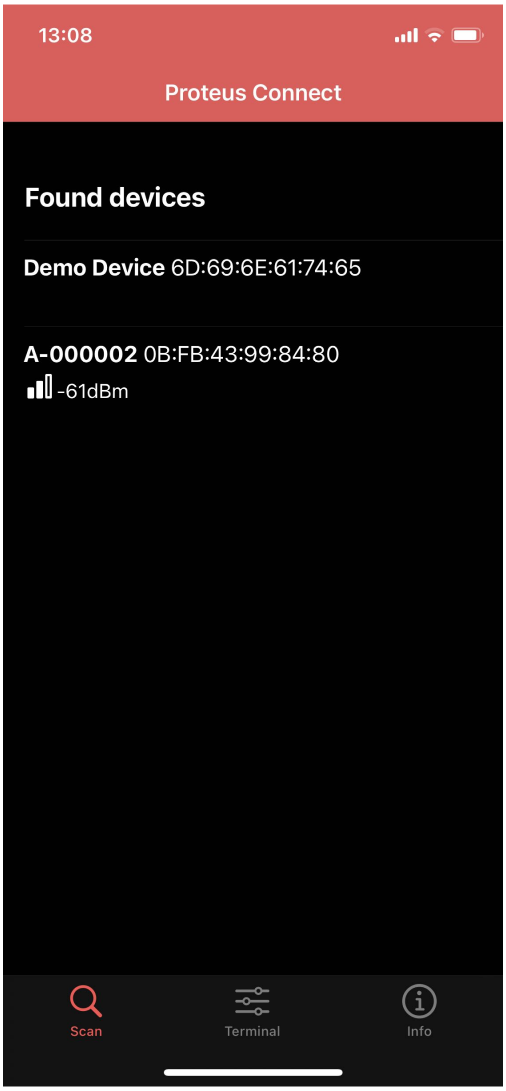
4.2 Smart phone using Proteus Connect app as central device

This chapter describes how to setup a connection to the Proteus radio module in peripheral mode (factory state), when a smart phone and the Proteus Connect App are used.

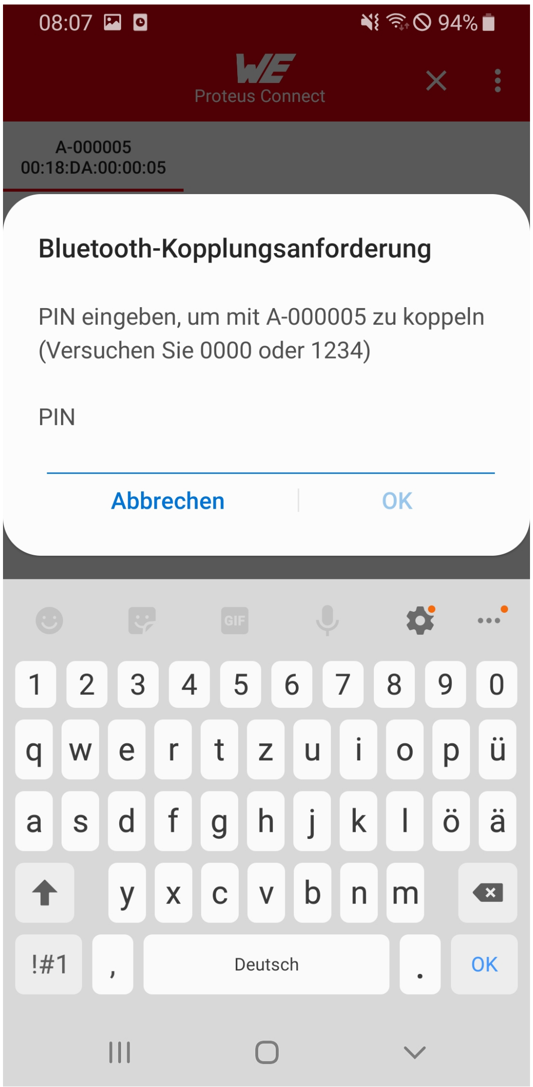
The Proteus Connect App [1] (for iOS and Android) is provided by Würth Elektronik eiSos as executable as well as source code.

Please perform the following steps:

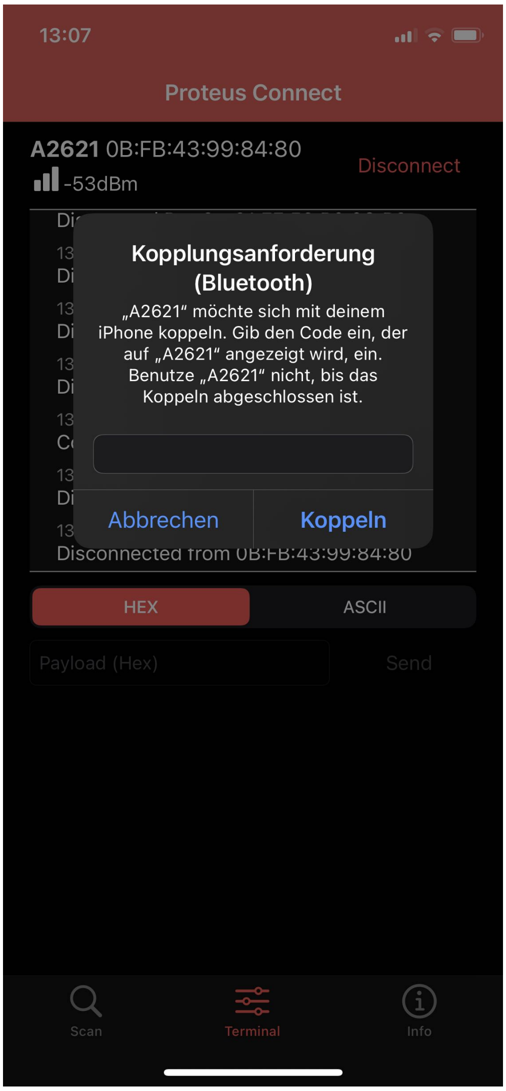
<table>
<tr><th>Android</th><th>iOS</th></tr>
<tr><td colspan="2">• Connect the module to a PC and open a terminal program using the Proteus default UART settings (115200 Baud, 8n1).
• Set the module into peripheral only mode as described in chapter 3.1. Initially, the module is advertising. Thus the Proteus <i>LED_1</i> is blinking.
• Start your smart phone, enable the Bluetooth® LE feature and start the Proteus Connect App.</td></tr>
</table>

Android	iOS
• Press "Scan" to find the module on the radio.  08:07 94% Select device Found devices Scan Default A-000005 00:18:DA:00:00:05 -63 dBm Scan Terminal Info	 13:08 Proteus Connect Found devices **Demo Device** 6D:69:6E:61:74:65 **A-000002** 0B:FB:43:99:84:80 -61dBm Scan Terminal Info

- When the module A-xxxxxx appears, press connect. (Note: the part after "A-" is the 3 LSB as ASCII hex of the BTMAC, the fixed part "0x0018DA" is not part of the device descriptor).
- As soon as the module has received the connection request the module *LED_1* (*LED_3* on the Proteus-EV) will constantly light up.

<table>
<tr><th>Android</th><th>iOS</th></tr>
<tr><td colspan="2">• Then the radio module requests for the static passkey. In default, the passkey is "123123".
• The Bluetooth® coupling requirement popup is shown in your smartphone.
• When the bonding feature is enabled in the authentication settings and the bonding information already exists, a re-entering of the passkey is not required when reconnecting.</td></tr>
<tr><td>
Bluetooth-Kopplungsanforderung
PIN eingeben, um mit A-000005 zu koppeln (Versuchen Sie 0000 oder 1234)
PIN

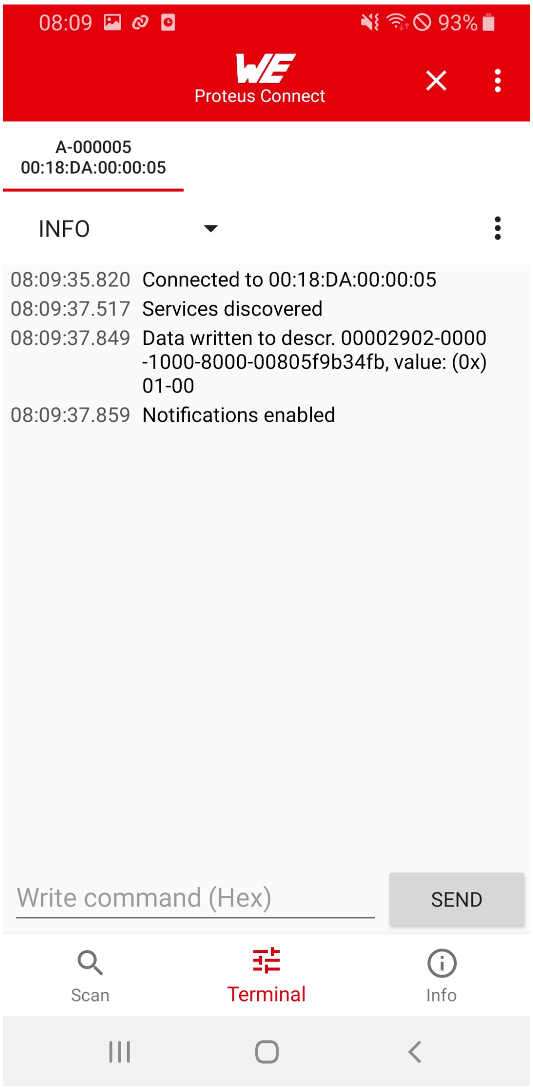
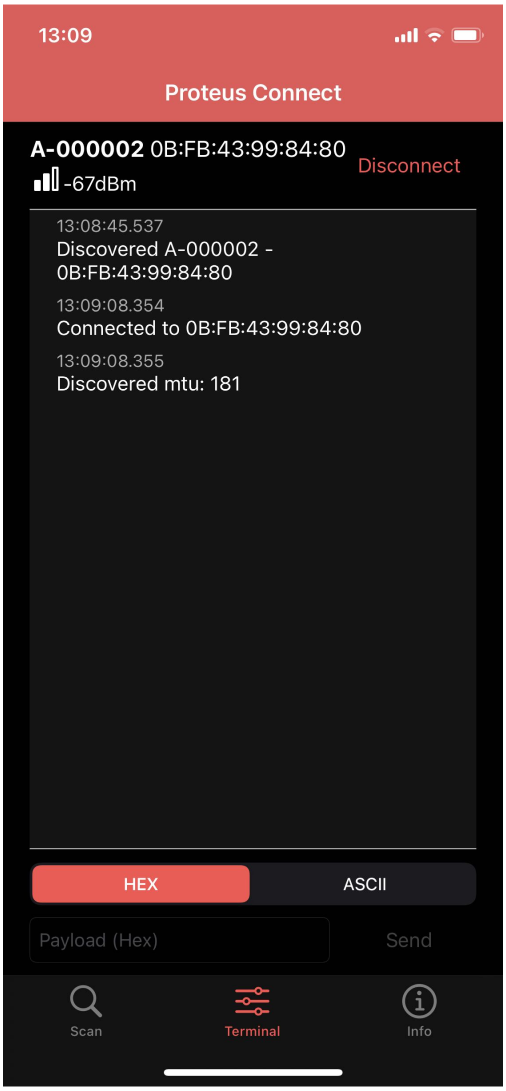
08:07
94%
Proteus Connect
A-000005
00:18:DA:00:00:05
Abbrechen
OK
1 2 3 4 5 6 7 8 9 0
q w e r t z u i o p ü
a s d f g h j k l ö ä
y x c v b n m
!#1
Deutsch
OK

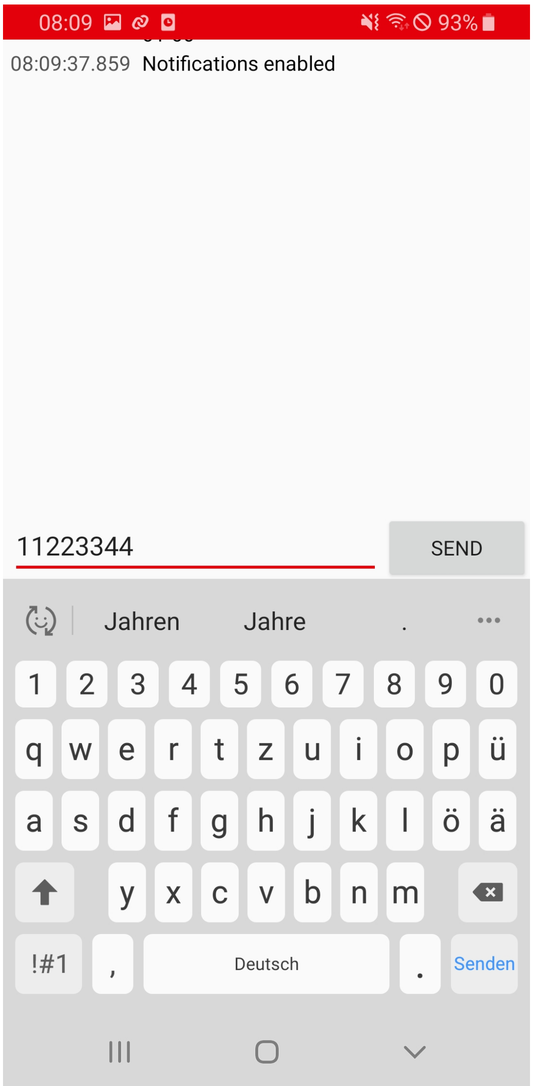
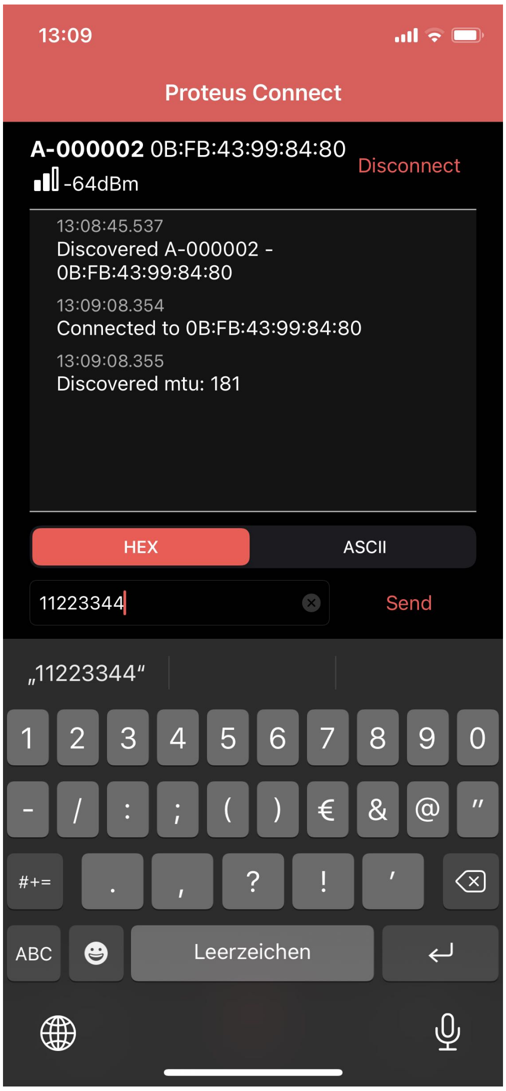
</td><td>
Kopplungsanforderung (Bluetooth)
„A2621“ möchte sich mit deinem iPhone koppeln. Gib den Code ein, der auf „A2621“ angezeigt wird, ein. Benutze „A2621“ nicht, bis das Koppeln abgeschlossen ist.
A2621 0B:FB:43:99:84:80
-53dBm
Disconnected from 0B:FB:43:99:84:80

13:07
Proteus Connect
Disconnect
Abbrechen
Koppeln
HEX
ASCII
Payload (Hex)
Send
Scan
Terminal
Info

</td></tr>
</table>

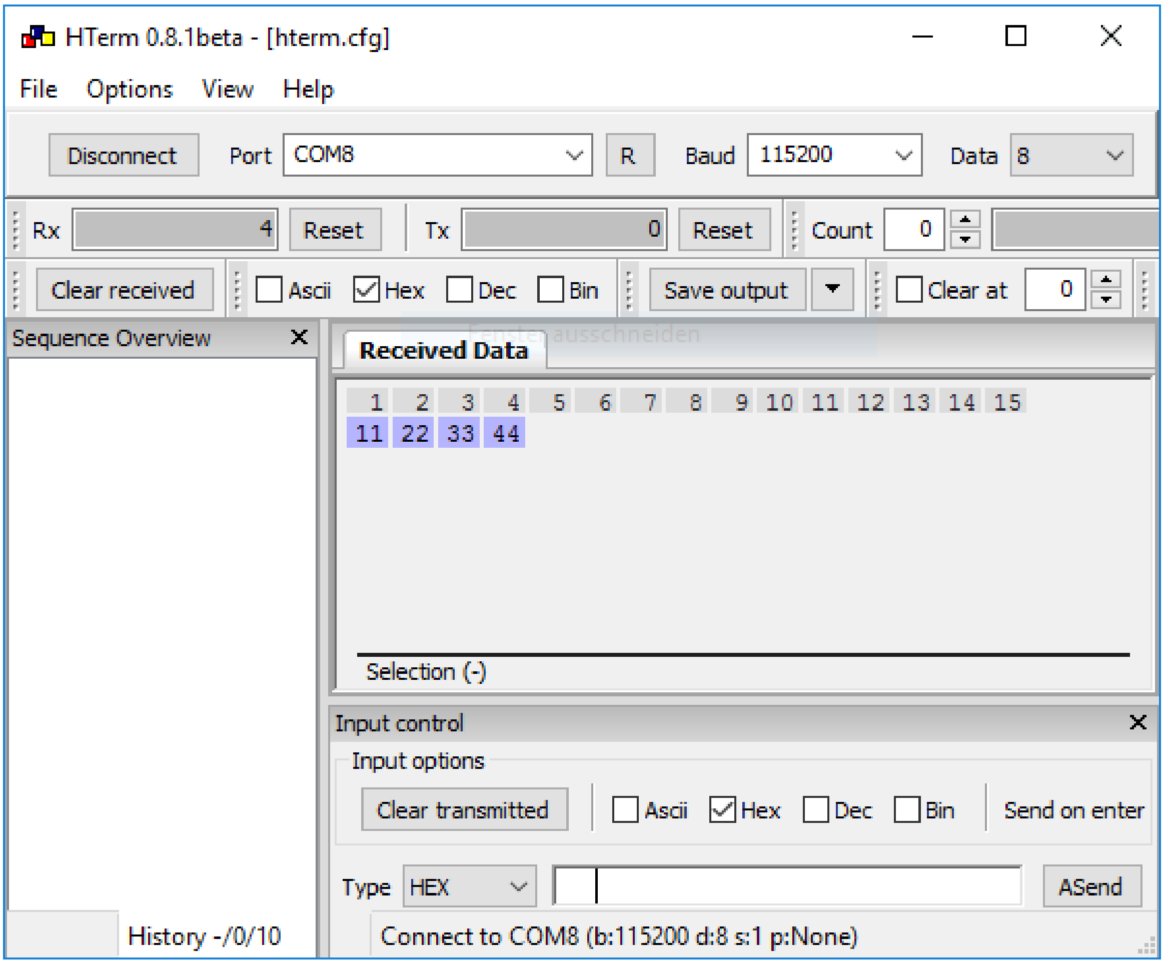
In few cases the Android may show an "authentication timeout" pop-up message, when entering the key. In this case, please proceed entering the key and simply do a reconnect. On this reconnect, the entered key information is reused and the connection is opened.

Android	iOS
• Now you are authenticated and the *LED_2* (*LED_2* on the Proteus-EV) is turned on. Now data can be transmitted in both directions.	
 08:09:35.820 Connected to 00:18:DA:00:00:05 08:09:37.517 Services discovered 08:09:37.849 Data written to descr. 00002902-0000-1000-8000-00805f9b34fb, value: (0x) 01-00 08:09:37.859 Notifications enabled	 A-000002 0B:FB:43:99:84:80 -67dBm 13:08:45.537 Discovered A-000002 - 0B:FB:43:99:84:80 13:09:08.354 Connected to 0B:FB:43:99:84:80 13:09:08.355 Discovered mtu: 181

<table>
<tr><th>Android</th><th>iOS</th></tr>
<tr><td colspan="2">• First of all, we want to send data from the smart phone to the radio module. To do so, enter your payload (for example 0x11 0x22 0x33 0x44) and press "SEND". The allowed payload size is dependent on the MTU that was negotiated in the connection process. The smallest supported MTU for all Bluetooth® 4.0 (or newer) devices results in a max payload of 19 bytes.</td></tr>
<tr><td>• Android usually allows up to 243 bytes.

08:09 93%
08:09:37.859 Notifications enabled
11223344
SEND</td><td>• iOS usually allows up to 181 bytes

13:09
Proteus Connect
A-000002 0B:FB:43:99:84:80 Disconnect
-64dBm
13:08:45.537
Discovered A-000002 - 0B:FB:43:99:84:80
13:09:08.354
Connected to 0B:FB:43:99:84:80
13:09:08.355
Discovered mtu: 181
HEX ASCII
11223344 Send
„11223344“</td></tr>
</table>

<table>
<tr><th>Android</th><th>iOS</th></tr>
<tr><td colspan="2">

- The payload that has been sent via radio is output by the Proteus via UART. In peripheral only mode, a transparent UART interface is used. This means, that only payload data is transmitted, without any packet header or footer. Thus the transmitted bytes 0x11 0x22 0x33 0x44 are displayed on the connected terminal program.



Port COM8 Baud 115200 Data 8

Rx 4 Tx 0 Count 0

□ Ascii ☑ Hex □ Dec □ Bin □ Clear at 0

```
 1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
11 22 33 44
```

Input options: □ Ascii ☑ Hex □ Dec □ Bin

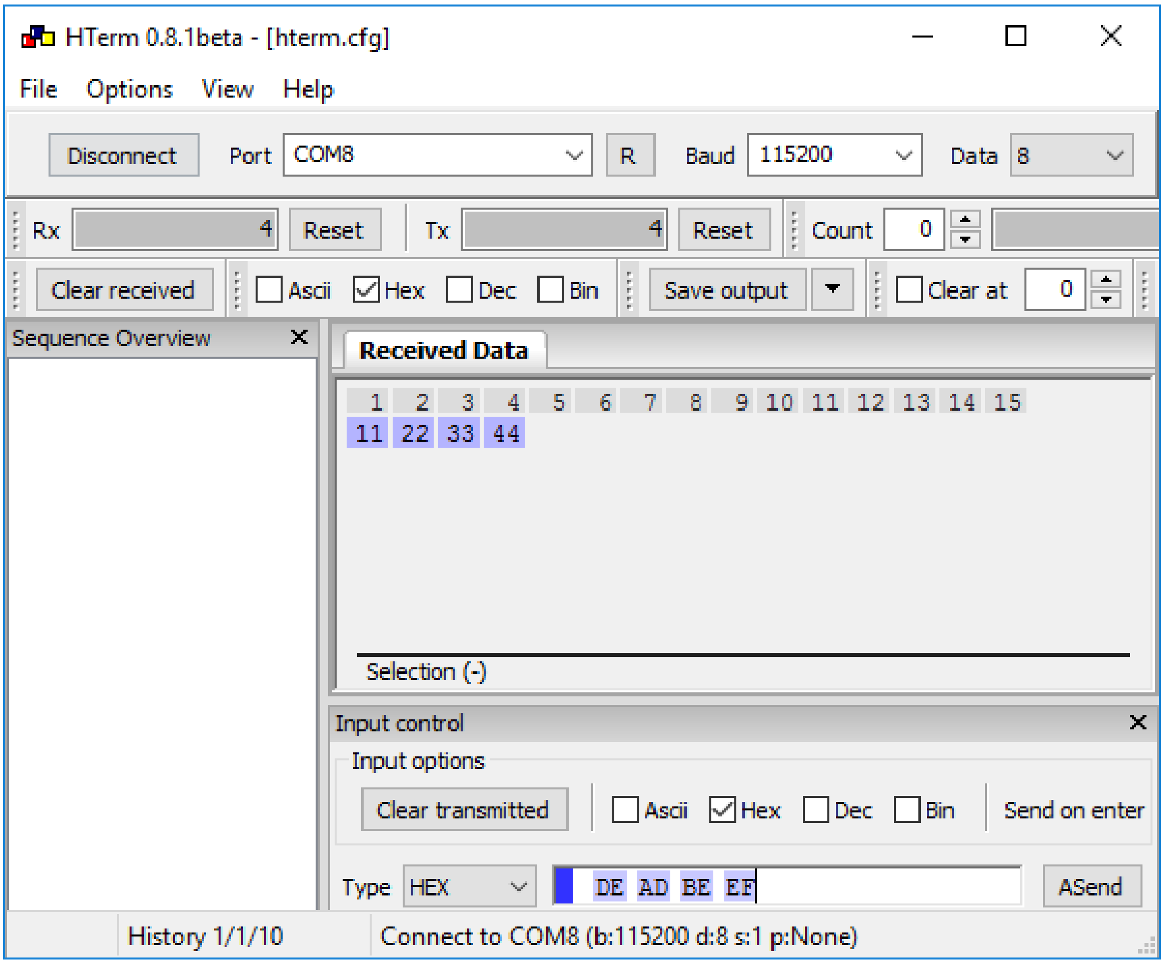
Type HEX

Connect to COM8 (b:115200 d:8 s:1 p:None)

</td></tr>
</table>

<table>
<tr><th>Android</th><th>iOS</th></tr>
<tr><td colspan="2">

- To send back data simply enter your payload in the respective terminal program field and press enter. In this example we choose 0xDE 0xAD 0xBE 0xEF. The header 0x01 will be automatically applied by the module and is not to be transmitted by the host.
- Here again the maximum payload size (MTU) must be respected.



Port COM8 Baud 115200 Data 8

Rx 4 Tx 4 Count 0

□ Ascii ☑ Hex □ Dec □ Bin □ Clear at 0

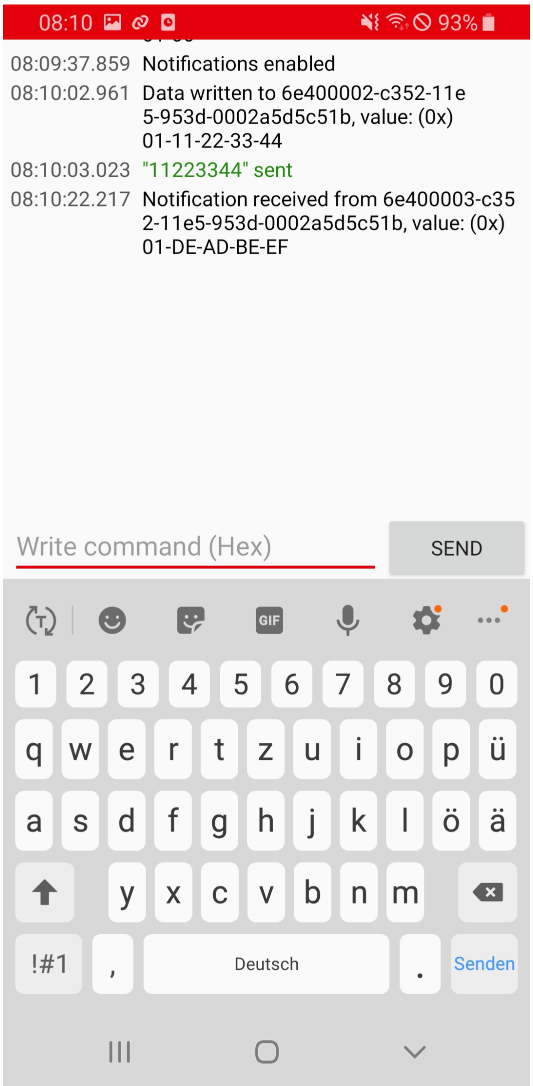
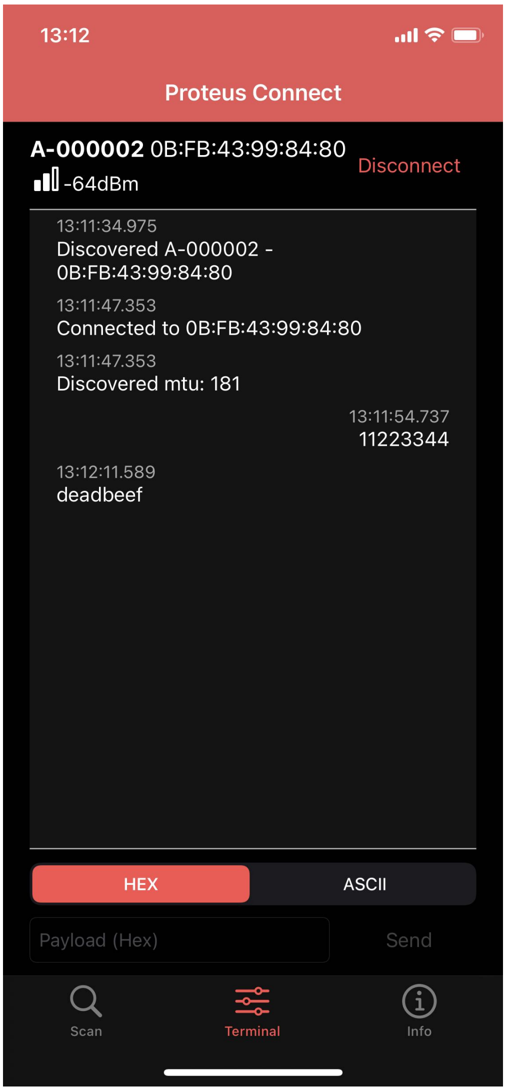
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
11 22 33 44

□ Ascii ☑ Hex □ Dec □ Bin

Type HEX DE AD BE EF

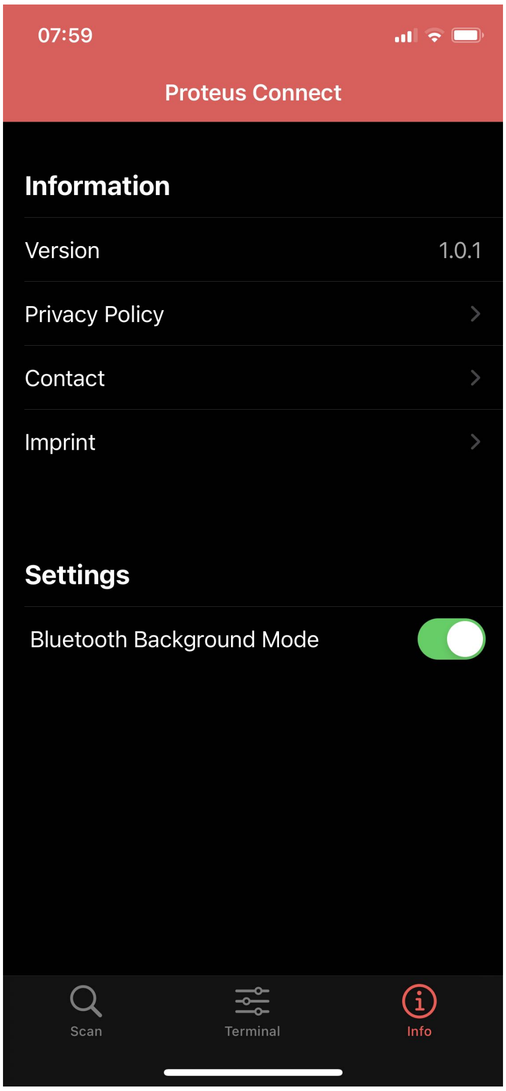
History 1/1/10 Connect to COM8 (b:115200 d:8 s:1 p:None)

</td></tr>
</table>

Android	iOS
- The received data is shown in the status window. It contains the header byte 0x01 and the payload 0xDE 0xAD 0xBE 0xEF, that has been entered in the terminal program.	- The received data is shown in the status window.
 08:10 93% 08:09:37.859 Notifications enabled 08:10:02.961 Data written to 6e400002-c352-11e5-953d-0002a5d5c51b, value: (0x) 01-11-22-33-44 08:10:03.023 "11223344" sent 08:10:22.217 Notification received from 6e400003-c352-11e5-953d-0002a5d5c51b, value: (0x) 01-DE-AD-BE-EF Write command (Hex) SEND GIF 1 2 3 4 5 6 7 8 9 0 q w e r t z u i o p ü a s d f g h j k l ö ä y x c v b n m !#1 , Deutsch . Senden	 13:12 Proteus Connect **A-000002** 0B:FB:43:99:84:80 Disconnect -64dBm 13:11:34.975 Discovered A-000002 - 0B:FB:43:99:84:80 13:11:47.353 Connected to 0B:FB:43:99:84:80 13:11:47.353 Discovered mtu: 181 13:11:54.737 11223344 13:12:11.589 deadbeef HEX ASCII Payload (Hex) Send

4.2.1 Background service on iOS

By default, iOS disconnects the Bluetooth® LE connection, in case the Proteus Connect App is put to background. To avoid this behavior, the background service of the Proteus Connect App must be enabled by going to the info tab and selecting the "Bluetooth Background Mode" slider.



07:59

Proteus Connect

Information

Version	1.0.1
Privacy Policy	
Contact	
Imprint	

Settings

Bluetooth Background Mode: on

Figure 6: Enable the background service on iOS

4.3 Proteus module or plug as central device

This chapter describes how to setup a connection to the Proteus radio module in peripheral mode (factory state), when another Proteus radio module or even Proteus plug is used as central device.

! For reasons of simplicity, we will call the Proteus radio module or plug, that is intended to setup the connection to the Proteus module running in peripheral only mode, **Proteus_central**. Furthermore, we will call the Proteus module running in peripheral only mode, **Proteus_peripheral**.

! Please note that the **Proteus_central** must run in command mode to initiate the connection setup.

! In this example we assume that the MAC of the **Proteus_peripheral** is 0x0018DA000011.

1. Configuring the correct security mode of the **Proteus_central**:
   The **Proteus_peripheral** uses the "static passkey pairing with bonding" as default security mode. As the central device must use the same security mode, the user setting `RF_SecFlags` of the **Proteus_central** must be also set to "static passkey with bonding" (0x0B = 11), before a connection setup can be done. To do so, please send the following command (`CMD_SET_REQ` with settings index 0x0C and value 0x0B) to the **Proteus_central**:

Info	**Proteus_central**	**Proteus_peripheral**
⇒ Request `CMD_SET_REQ` to set the right security mode of the **Proteus_central**	02 11 02 00 0C 0B 16	
⇐ Response `CMD_SET_CNF`: Setting successfully set	02 51 01 00 00 52	
⇐ Response `CMD_GETSTATE_CNF`: **Proteus_central** restarted	02 41 02 00 01 01 41	

   Now, the connection setup can be initiated.

2. Connect **Proteus_central** to the **Proteus_peripheral** via Bluetooth® LE.

Info	Proteus_central	Proteus_peripheral
⇒ Request CMD_CONNECT_REQ with FS_BTMAC of **Proteus_peripheral**	02 06 06 00 11 00 00 DA 18 00 D1	
⇐ Response CMD_CONNECT_CNF: Request understood, try to connect now	02 46 01 00 00 45	
⇐ Indication CMD_CONNECT_IND: Physical connection established successfully to the module with FS_BTMAC 0x11 0x00 0x00 0xDA 0x18 0x00	02 86 07 00 00 11 00 00 DA 18 00 50	

a) Option A: No bonding data available (i.e. when connecting for the first time). Pass key must be entered as soon as requested by the **Proteus_central** by a CMD_PASSKEY_IND message.

STOP In case the CMD_PASSKEY_IND message does not appear, but the Bluetooth® LE connection has been closed, the security settings of the **Proteus_central** do not match. Please check again the user setting RF_SecFlags of the **Proteus_central**, as described in step 1.

Info	Proteus_central	Proteus_peripheral
⇐ Indication CMD_PASSKEY_IND to ask for the pass key	02 8D 07 00 00 11 00 00 DA 18 00 5B	
⇒ Answer with the CMD_PASSKEY_REQ and the correct pass key (default is "123123")	02 0D 06 00 31 32 33 31 32 33 09	
⇐ Response CMD_PASSKEY_CNF: Pass key ok	02 4D 01 00 00 4E	
⇐ Indication CMD_SECURITY_IND, status 0x01 (encrypted link, bonding established), with FS_BTMAC 0x11 0x00 0x00 0xDA 0x18 0x00	02 88 07 00 01 11 00 00 DA 18 00 5F	
⇐ Indication CMD_CHANNELOPEN_RSP: Channel opened successfully to the module with FS_BTMAC 0x11 0x00 0x00 0xDA 0x18 0x00 and maximum payload size of 0xF3 (243 Bytes) per packet	02 C6 08 00 00 11 00 00 DA 18 00 F3 EC	

b) Option B: Bonding data is already available (i.e. when reconnecting). No pass key must be entered.

Info	Proteus_central	Proteus_peripheral
⇐ Indication CMD_SECURITY_IND, status 0x00 (encrypted link, bonding data already available), with FS_BTMAC 0x11 0x00 0x00 0xDA 0x18 0x00	02 88 07 00 00 11 00 00 DA 18 00 5E	
⇐ Indication CMD_CHANNELOPEN_RSP: Channel opened successfully to the module with FS_BTMAC 0x11 0x00 0x00 0xDA 0x18 0x00 and maximum payload size of 0xF3 (243 Bytes) per packet	02 C6 08 00 00 11 00 00 DA 18 00 F3 EC	

3. Now the connection is active. Thus data can be sent in each direction. Let us send a string "ABCD" from **Proteus_peripheral** to **Proteus_central**.

! The RSSI values will be different in your tests.

Info	Proteus_central	Proteus_peripheral
⇒ Transparent send "ABCD" to **Proteus_central**		41 42 43 44
⇐ Indication CMD_DATA_IND: Received string "ABCD" from FS_BTMAC 0x11 0x00 0x00 0xDA 0x18 0x00 with RSSI of 0xCA (-54dBm)	02 84 0B 00 11 00 00 DA 18 00 CA 41 42 43 44 90	

4. Reply with "EFGH" to the **Proteus_peripheral**.

Info	Proteus_central	Proteus_peripheral
⇒ Request CMD_DATA_REQ: Send "EFGH" to **Proteus_peripheral**	02 04 04 00 45 46 47 48 0E	
⇐ Response CMD_DATA_CNF: Request received, send data now	02 44 01 00 00 47	
⇐ Transparent received string "EFGH"		45 46 47 48
⇐ Response CMD_TXCOMPLETE_RSP: Data transmitted successfully	02 C4 01 00 00 C7	

5. Now **Proteus_central** closes the connection.

Info	Proteus_central	Proteus_peripheral
⇒ Request CMD_DISCONNECT_REQ: Disconnect	02 07 00 00 05	
⇐ Response CMD_DISCONNECT_CNF: Request received, disconnect now	02 47 01 00 00 44	
⇐ Indication CMD_DISCONNECT_IND: Connection closed	02 87 01 00 16 92	

5 References

[1] Source codes of Proteus Connect App
https://github.com/WurthElektronik/Proteus-Connect-Android
https://github.com/WurthElektronik/Proteus-Connect-iOS

6 Important notes

The following conditions apply to all goods within the wireless connectivity product range of Würth Elektronik eiSos GmbH & Co. KG:

6.1 General customer responsibility

Some goods within the product range of Würth Elektronik eiSos GmbH & Co. KG contain statements regarding general suitability for certain application areas. These statements about suitability are based on our knowledge and experience of typical requirements concerning the areas, serve as general guidance and cannot be estimated as binding statements about the suitability for a customer application. The responsibility for the applicability and use in a particular customer design is always solely within the authority of the customer. Due to this fact, it is up to the customer to evaluate, where appropriate to investigate and to decide whether the device with the specific product characteristics described in the product specification is valid and suitable for the respective customer application or not. Accordingly, the customer is cautioned to verify that the documentation is current before placing orders.

6.2 Customer responsibility related to specific, in particular safety-relevant applications

It has to be clearly pointed out that the possibility of a malfunction of electronic components or failure before the end of the usual lifetime cannot be completely eliminated in the current state of the art, even if the products are operated within the range of the specifications. The same statement is valid for all software sourcecode and firmware parts contained in or used with or for products in the wireless connectivity and sensor product range of Würth Elektronik eiSos GmbH & Co. KG. In certain customer applications requiring a high level of safety and especially in customer applications in which the malfunction or failure of an electronic component could endanger human life or health, it must be ensured by most advanced technological aid of suitable design of the customer application that no injury or damage is caused to third parties in the event of malfunction or failure of an electronic component.

6.3 Best care and attention

Any product-specific data sheets, manuals, application notes, PCN's, warnings and cautions must be strictly observed in the most recent versions and matching to the products firmware revisions. This documents can be downloaded from the product specific sections on the wireless connectivity homepage.

6.4 Customer support for product specifications

Some products within the product range may contain substances, which are subject to restrictions in certain jurisdictions in order to serve specific technical requirements. Necessary information is available on request. In this case, the field sales engineer or the internal sales person in charge should be contacted who will be happy to support in this matter.

6.5 Product improvements

Due to constant product improvement, product specifications may change from time to time. As a standard reporting procedure of the Product Change Notification (PCN) according to the JEDEC-Standard, we inform about major changes. In case of further queries regarding the PCN, the field sales engineer, the internal sales person or the technical support team in charge should be contacted. The basic responsibility of the customer as per section 6.1 and 6.2 remains unaffected. All wireless connectivity module driver software ¨wireless connectivity SDK¨ and it's source codes as well as all PC software tools are not subject to the Product Change Notification information process.

6.6 Product life cycle

Due to technical progress and economical evaluation we also reserve the right to discontinue production and delivery of products. As a standard reporting procedure of the Product Termination Notification (PTN) according to the JEDEC-Standard we will inform at an early stage about inevitable product discontinuance. According to this, we cannot ensure that all products within our product range will always be available. Therefore, it needs to be verified with the field sales engineer or the internal sales person in charge about the current product availability expectancy before or when the product for application design-in disposal is considered. The approach named above does not apply in the case of individual agreements deviating from the foregoing for customer-specific products.

6.7 Property rights

All the rights for contractual products produced by Würth Elektronik eiSos GmbH & Co. KG on the basis of ideas, development contracts as well as models or templates that are subject to copyright, patent or commercial protection supplied to the customer will remain with Würth Elektronik eiSos GmbH & Co. KG. Würth Elektronik eiSos GmbH & Co. KG does not warrant or represent that any license, either expressed or implied, is granted under any patent right, copyright, mask work right, or other intellectual property right relating to any combination, application, or process in which Würth Elektronik eiSos GmbH & Co. KG components or services are used.

6.8 General terms and conditions

Unless otherwise agreed in individual contracts, all orders are subject to the current version of the "General Terms and Conditions of Würth Elektronik eiSos Group", last version available at *www.we-online.com*.

7 Legal notice

7.1 Exclusion of liability

Würth Elektronik eiSos GmbH & Co. KG considers the information in this document to be correct at the time of publication. However, Würth Elektronik eiSos GmbH & Co. KG reserves the right to modify the information such as technical specifications or functions of its products or discontinue the production of these products or the support of one of these products without any written announcement or notification to customers. The customer must make sure that the information used corresponds to the latest published information. Würth Elektronik eiSos GmbH & Co. KG does not assume any liability for the use of its products. Würth Elektronik eiSos GmbH & Co. KG does not grant licenses for its patent rights or for any other of its intellectual property rights or third-party rights.

Notwithstanding anything above, Würth Elektronik eiSos GmbH & Co. KG makes no representations and/or warranties of any kind for the provided information related to their accuracy, correctness, completeness, usage of the products and/or usability for customer applications. Information published by Würth Elektronik eiSos GmbH & Co. KG regarding third-party products or services does not constitute a license to use such products or services or a warranty or endorsement thereof.

7.2 Suitability in customer applications

The customer bears the responsibility for compliance of systems or units, in which Würth Elektronik eiSos GmbH & Co. KG products are integrated, with applicable legal regulations. Customer acknowledges and agrees that it is solely responsible for compliance with all legal, regulatory and safety-related requirements concerning its products, and any use of Würth Elektronik eiSos GmbH & Co. KG components in its applications, notwithstanding any applications-related in-formation or support that may be provided by Würth Elektronik eiSos GmbH & Co. KG. Customer represents and agrees that it has all the necessary expertise to create and implement safeguards which anticipate dangerous consequences of failures, monitor failures and their consequences lessen the likelihood of failures that might cause harm and take appropriate remedial actions. The customer will fully indemnify Würth Elektronik eiSos GmbH & Co. KGand its representatives against any damages arising out of the use of any Würth Elektronik eiSos GmbH & Co. KG components in safety-critical applications.

7.3 Trademarks

AMBER wireless is a registered trademark of Würth Elektronik eiSos GmbH & Co. KG. All other trademarks, registered trademarks, and product names are the exclusive property of the respective owners.

7.4 Usage restriction

Würth Elektronik eiSos GmbH & Co. KG products have been designed and developed for usage in general electronic equipment only. This product is not authorized for use in equipment where a higher safety standard and reliability standard is especially required or where a failure of the product is reasonably expected to cause severe personal injury or death, unless the parties have executed an agreement specifically governing such use. Moreover, Würth Elektronik eiSos GmbH & Co. KG products are neither designed nor intended for use in areas such as military, aerospace, aviation, nuclear control, submarine, transportation (automotive control, train control, ship control), transportation signal, disaster prevention, medical, public information network etc. Würth Elektronik eiSos GmbH & Co. KG must be informed about the intent of such usage before the design-in stage. In addition, sufficient reliability evaluation checks for safety must be performed on every electronic component, which is used in electrical circuits that require high safety and reliability function or performance. By using Würth Elektronik eiSos GmbH & Co. KG products, the customer agrees to these terms and conditions.

8 License terms

This License Terms will take effect upon the purchase and usage of the Würth Elektronik eiSos GmbH & Co. KG wireless connectivity products. You hereby agree that this license terms is applicable to the product and the incorporated software, firmware and source codes (collectively, "Software") made available by Würth Elektronik eiSos in any form, including but not limited to binary, executable or source code form.
The software included in any Würth Elektronik eiSos wireless connectivity product is purchased to you on the condition that you accept the terms and conditions of this license terms. You agree to comply with all provisions under this license terms.

8.1 Limited license

Würth Elektronik eiSos hereby grants you a limited, non-exclusive, non-transferable and royalty-free license to use the software and under the conditions that will be set forth in this license terms. You are free to use the provided Software only in connection with one of the products from Würth Elektronik eiSos to the extent described in this license terms. You are entitled to change or alter the source code for the sole purpose of creating an application embedding the Würth Elektronik eiSos wireless connectivity product. The transfer of the source code to third parties is allowed to the sole extent that the source code is used by such third parties in connection with our product or another hardware provided by Würth Elektronik eiSos under strict adherence of this license terms. Würth Elektronik eiSos will not assume any liability for the usage of the incorporated software and the source code. You are not entitled to transfer the source code in any form to third parties without prior written consent of Würth Elektronik eiSos.
You are not allowed to reproduce, translate, reverse engineer, decompile, disassemble or create derivative works of the incorporated Software and the source code in whole or in part. No more extensive rights to use and exploit the products are granted to you.

8.2 Usage and obligations

The responsibility for the applicability and use of the Würth Elektronik eiSos wireless connectivity product with the incorporated Firmware in a particular customer design is always solely within the authority of the customer. Due to this fact, it is up to you to evaluate and investigate, where appropriate, and to decide whether the device with the specific product characteristics described in the product specification is valid and suitable for your respective application or not.
You are responsible for using the Würth Elektronik eiSos wireless connectivity product with the incorporated Firmware in compliance with all applicable product liability and product safety laws. You acknowledge to minimize the risk of loss and harm to individuals and bear the risk for failure leading to personal injury or death due to your usage of the product.
Würth Elektronik eiSos' products with the incorporated Firmware are not authorized for use in safety-critical applications, or where a failure of the product is reasonably expected to cause severe personal injury or death. Moreover, Würth Elektronik eiSos' products with the incorporated Firmware are neither designed nor intended for use in areas such as military, aerospace, aviation, nuclear control, submarine, transportation (automotive control, train control, ship control), transportation signal, disaster prevention, medical, public information network etc. You shall inform Würth Elektronik eiSos about the intent of such usage before design-in stage. In certain customer applications requiring a very high level of safety and in which the malfunction or failure of an electronic component could endanger human life or

health, you must ensure to have all necessary expertise in the safety and regulatory ramifications of your applications. You acknowledge and agree that you are solely responsible for all legal, regulatory and safety-related requirements concerning your products and any use of Würth Elektronik eiSos' products with the incorporated Firmware in such safety-critical applications, notwithstanding any applications-related information or support that may be provided by Würth Elektronik eiSos. YOU SHALL INDEMNIFY WÜRTH ELEKTRONIK EISOS AGAINST ANY DAMAGES ARISING OUT OF THE USE OF WÜRTH ELEKTRONIK EISOS' PRODUCTS WITH THE INCORPORATED FIRMWARE IN SUCH SAFETY-CRITICAL APPLICATIONS.

8.3 Ownership

The incorporated Firmware created by Würth Elektronik eiSos is and will remain the exclusive property of Würth Elektronik eiSos.

8.4 Firmware update(s)

You have the opportunity to request the current and actual Firmware for a bought wireless connectivity Product within the time of warranty. However, Würth Elektronik eiSos has no obligation to update a modules firmware in their production facilities, but can offer this as a service on request. The upload of firmware updates falls within your responsibility, e.g. via ACC or another software for firmware updates. Firmware updates will not be communicated automatically. It is within your responsibility to check the current version of a firmware in the latest version of the product manual on our website. The revision table in the product manual provides all necessary information about firmware updates. There is no right to be provided with binary files, so called "Firmware images", those could be flashed through JTAG, SWD, Spi-Bi-Wire, SPI or similar interfaces.

8.5 Disclaimer of warranty

THE FIRMWARE IS PROVIDED "AS IS". YOU ACKNOWLEDGE THAT WÜRTH ELEKTRONIK EISOS MAKES NO REPRESENTATIONS AND WARRANTIES OF ANY KIND RELATED TO, BUT NOT LIMITED TO THE NON-INFRINGEMENT OF THIRD PARTIES' INTELLECTUAL PROPERTY RIGHTS OR THE MERCHANTABILITY OR FITNESS FOR YOUR INTENDED PURPOSE OR USAGE. WÜRTH ELEKTRONIK EISOS DOES NOT WARRANT OR REPRESENT THAT ANY LICENSE, EITHER EXPRESS OR IMPLIED, IS GRANTED UNDER ANY PATENT RIGHT, COPYRIGHT, MASK WORK RIGHT, OR OTHER INTELLECTUAL PROPERTY RIGHT RELATING TO ANY COMBINATION, MACHINE, OR PROCESS IN WHICH THE WÜRTH ELEKTRONIK EISOS' PRODUCT WITH THE INCORPORATED FIRMWARE IS USED. INFORMATION PUBLISHED BY WÜRTH ELEKTRONIK EISOS REGARDING THIRD-PARTY PRODUCTS OR SERVICES DOES NOT CONSTITUTE A LICENSE FROM WÜRTH ELEKTRONIK EISOS TO USE SUCH PRODUCTS OR SERVICES OR A WARRANTY OR ENDORSEMENT THEREOF.

8.6 Limitation of liability

Any liability not expressly provided by Würth Elektronik eiSos shall be disclaimed.
You agree to hold us harmless from any third-party claims related to your usage of the Würth Elektronik eiSos' products with the incorporated Firmware, software and source code. Würth

Elektronik eiSos disclaims any liability for any alteration, development created by you or your customers as well as for any combination with other products.

8.7 Applicable law and jurisdiction

Applicable law to this license terms shall be the laws of the Federal Republic of Germany. Any dispute, claim or controversy arising out of or relating to this license terms shall be resolved and finally settled by the court competent for the location of Würth Elektronik eiSos' registered office.

8.8 Severability clause

If a provision of this license terms is or becomes invalid, unenforceable or null and void, this shall not affect the remaining provisions of the terms. The parties shall replace any such provisions with new valid provisions that most closely approximate the purpose of the terms.

8.9 Miscellaneous

Würth Elektronik eiSos reserves the right at any time to change this terms at its own discretion. It is your responsibility to check at Würth Elektronik eiSos homepage for any updates. Your continued usage of the products will be deemed as the acceptance of the change.
We recommend you to be updated about the status of new firmware and software, which is available on our website or in our data sheet and manual, and to implement new software in your device where appropriate.
By ordering a wireless connectivity product, you accept this license terms in all terms.

List of Figures

List of Tables

WÜRTH ELEKTRONIK

more than you expect

Internet of Things

Monitoring & Control

Automated Meter Reading

Contact:
Würth Elektronik eiSos GmbH & Co. KG
Division Wireless Connectivity & Sensors

Max-Eyth-Straße 1
74638 Waldenburg
Germany

Tel.: +49 651 99355-0
Fax.: +49 651 99355-69
www.we-online.com/wireless-connectivity