



ANR004 PROTEUS

HOW TO USE THE PERIPHERAL ONLY MODE

VERSION 2.3

JANUARY 3, 2020

Revision history

Manual version	Notes	Date
1.0	<ul style="list-style-type: none"> Initial version 	February 2017
1.1	<ul style="list-style-type: none"> Updated MTU size to 247 bytes 	July 2017
2.0	<ul style="list-style-type: none"> New corporate design 	June 2018
2.1	<ul style="list-style-type: none"> Updated product name from AMB2621 to Proteus-I 	November 2018
2.2	<ul style="list-style-type: none"> Updated file name to new AppNote name structure. Updated important notes, legal notice & license terms chapters. 	June 2019
2.3	<ul style="list-style-type: none"> Added Proteus-II and Proteus-III description Updated address of Division Wireless Connectivity & Sensors location 	January 2020

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	4
2	Prerequisites	5
3	Peripheral only mode	6
3.1	How to set the Proteus radio module to peripheral only mode?	6
3.2	Connection setup information	8
3.3	Connection setup example using the nRF Connect App	10
4	Preconfiguring of the module	19
5	Important notes	20
5.1	General customer responsibility	20
5.2	Customer responsibility related to specific, in particular safety-relevant applications	20
5.3	Best care and attention	20
5.4	Customer support for product specifications	20
5.5	Product improvements	21
5.6	Product life cycle	21
5.7	Property rights	21
5.8	General terms and conditions	21
6	Legal notice	22
6.1	Exclusion of liability	22
6.2	Suitability in customer applications	22
6.3	Trademarks	22
6.4	Usage restriction	22
7	License terms	24
7.1	Limited license	24
7.2	Usage and obligations	24
7.3	Ownership	25
7.4	Firmware update(s)	25
7.5	Disclaimer of warranty	25
7.6	Limitation of liability	26
7.7	Applicable law and jurisdiction	26
7.8	Severability clause	26
7.9	Miscellaneous	26

1 Introduction

The Proteus is a Bluetooth® module based on the nRF52 Nordic Semiconductors SoC which presents various Bluetooth® LE and low power features.

In addition to the standard command mode, that uses commands to run and configure the 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 configuration(s) 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 module. These steps are described with help of the nRF Connect App which is an open source App providing standard Bluetooth® LE functions for iOS as well as for Android devices.

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.
- Smart phone with Bluetooth® LE function and the Nordic Semiconductor nRF Connect App



Figure 1: Proteus-I evaluation board with USB cable

3 Peripheral only mode

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 (see Proteus advanced developer guide) is of advantage.

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 of less than 1ms.



After start-up 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*.

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

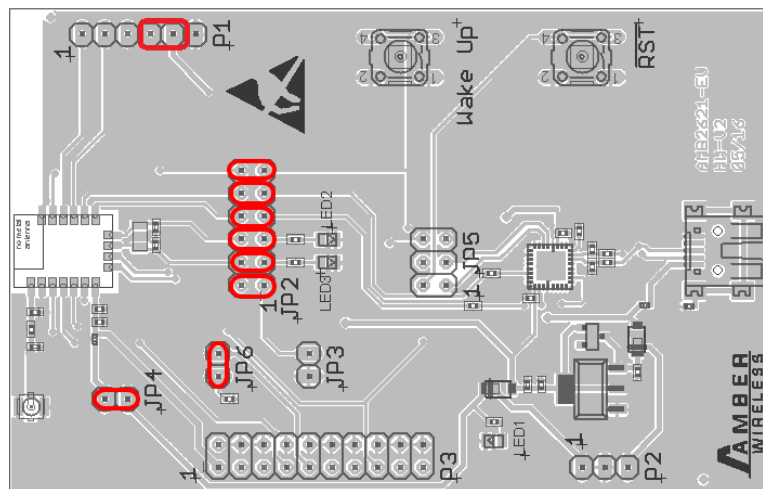


Figure 2: On Proteus-I and Proteus-II evaluation board, set these jumpers to start the peripheral only mode after reset.

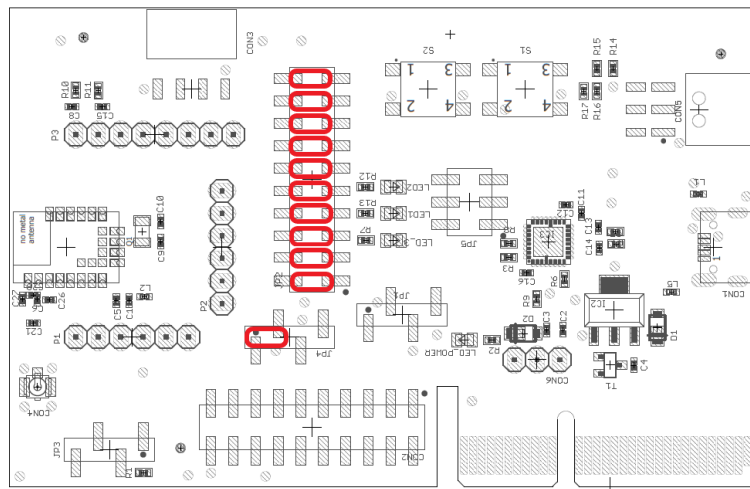


Figure 3: On Proteus-III evaluation board, set these jumpers to start the peripheral only mode after reset.

3.2 Connection setup information

In factory state the peripheral only mode uses the static passkey pairing authentication method, which requests a static passkey from the connecting device. Figure 4 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.



If the security level of the central device is lower than the security mode of the peripheral, the central cannot access the peripheral's characteristics. In this case, the central sends the notification enable message, which is ignored by the peripheral. Thus, the central signalizes an open connection, although it does not have access to the peripheral and thus data cannot be transmitted!

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® 4.0 default MTU which results in 19 bytes payload for the user but will be compatible to pre Bluetooth® 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 4.

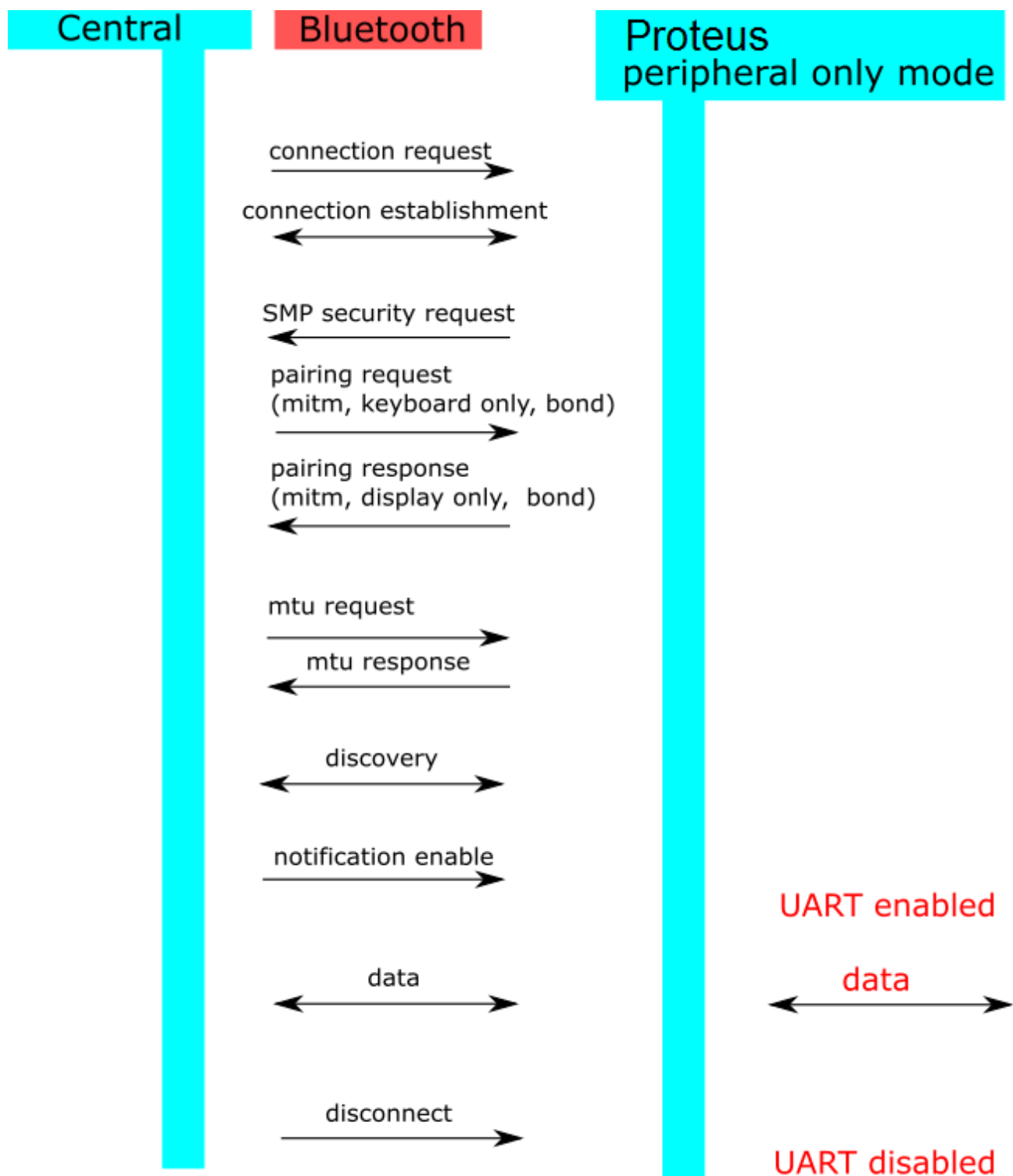
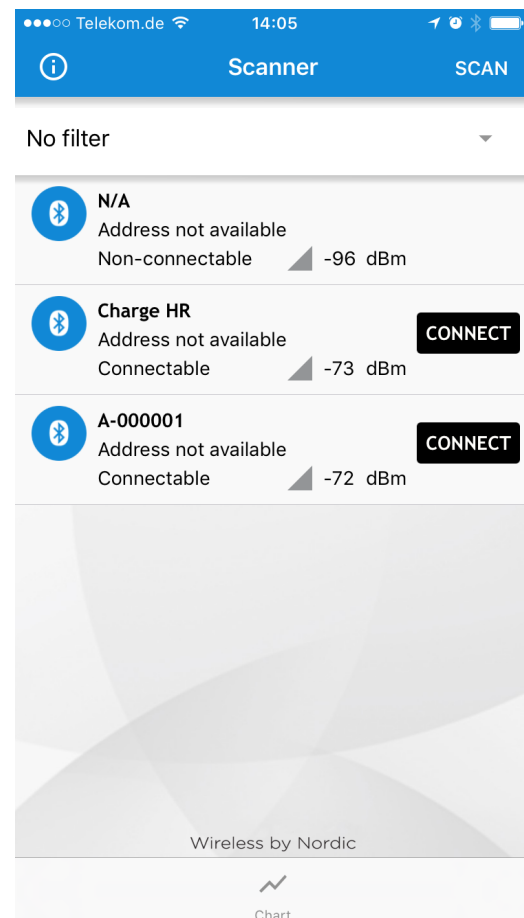
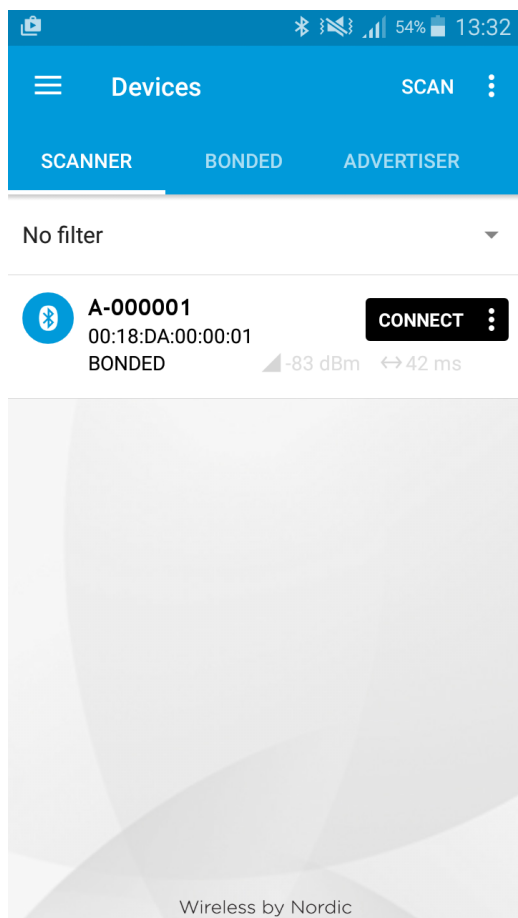


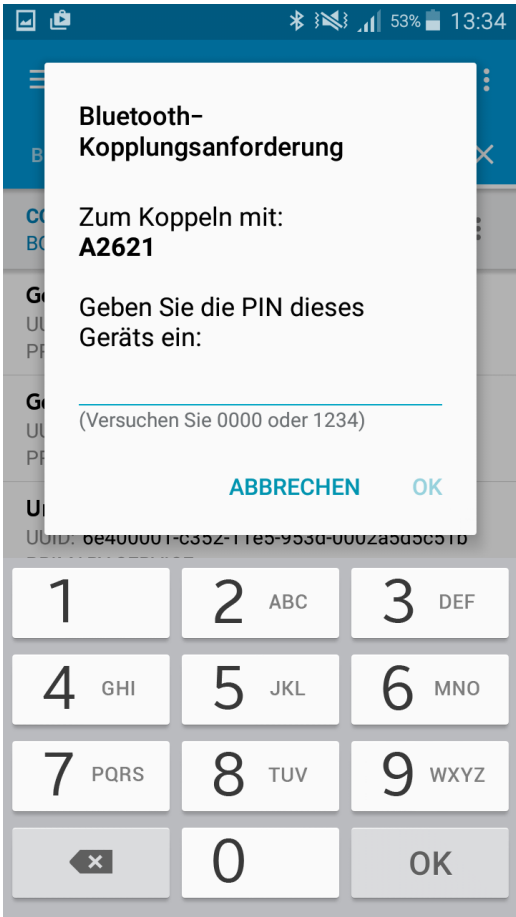
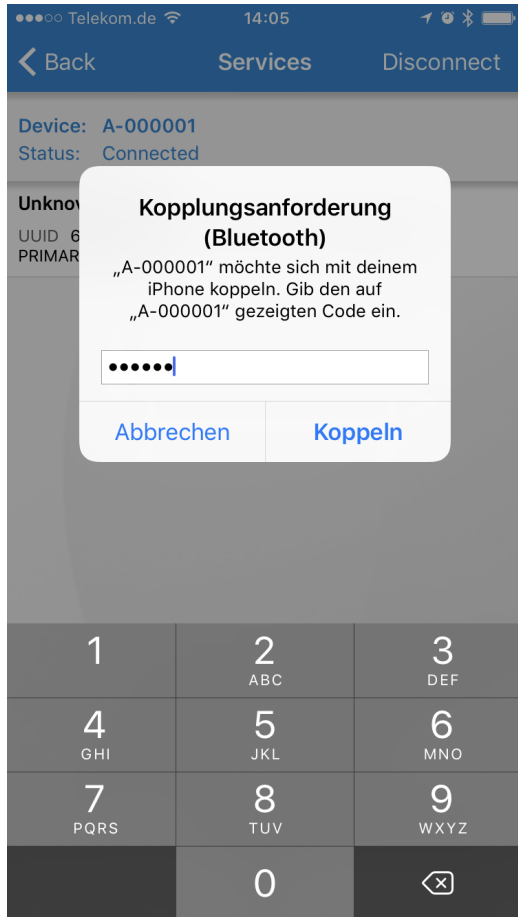
Figure 4: Steps for the connection setup in static passkey mode (default)

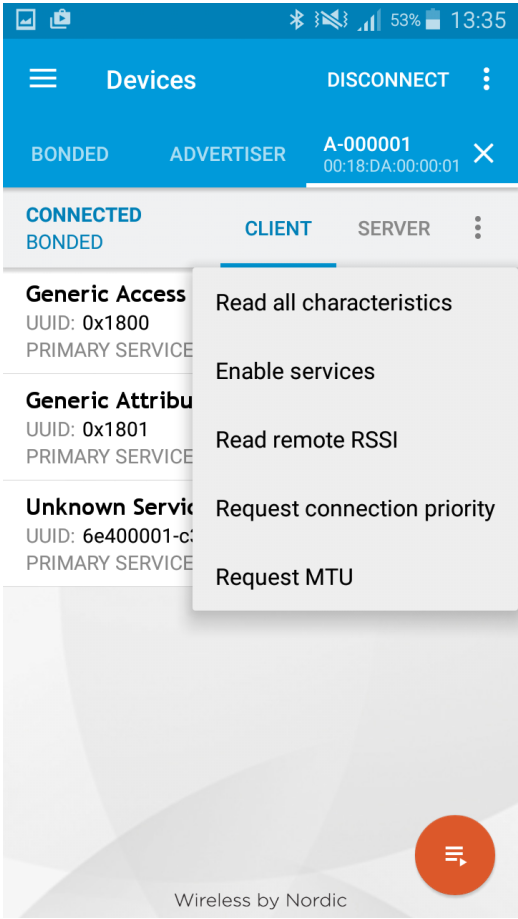
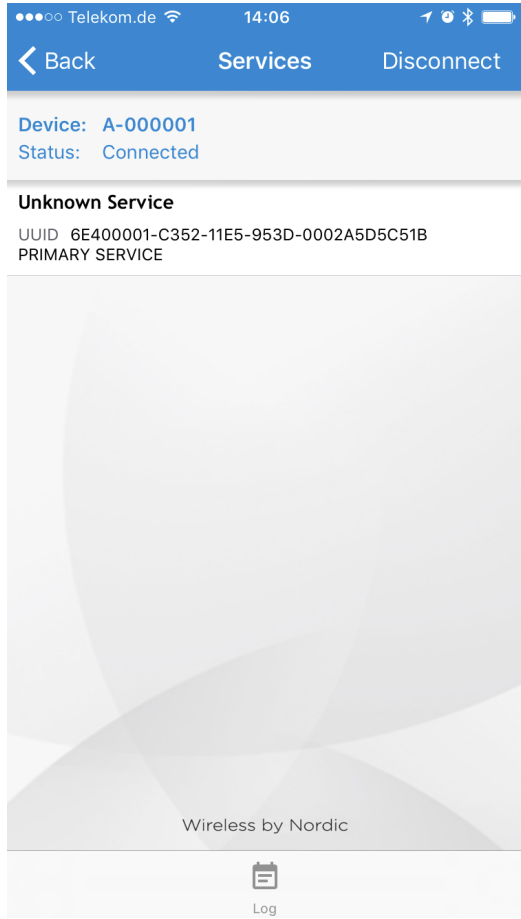
3.3 Connection setup example using the nRF Connect App

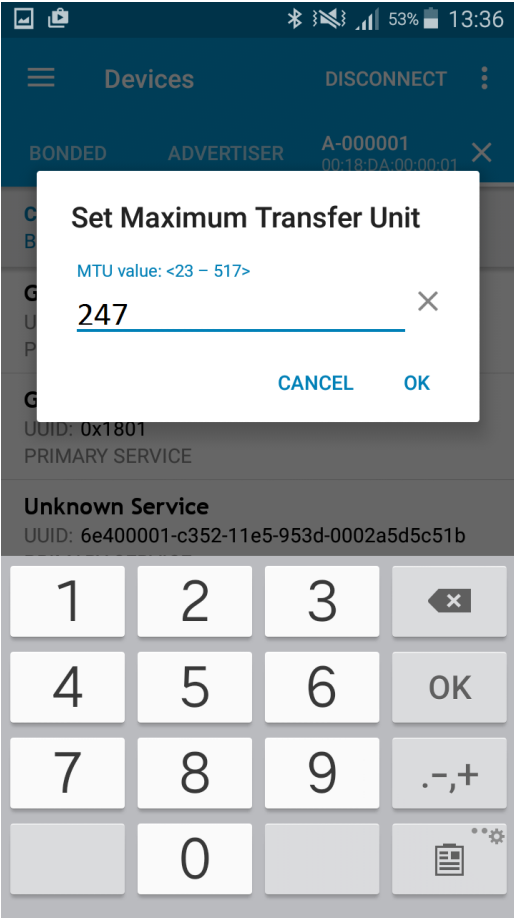
This chapter describes how to setup a connection to the Proteus in peripheral mode (factory state), when a smart phone and the nRF Connect App are used. Please perform the following steps:

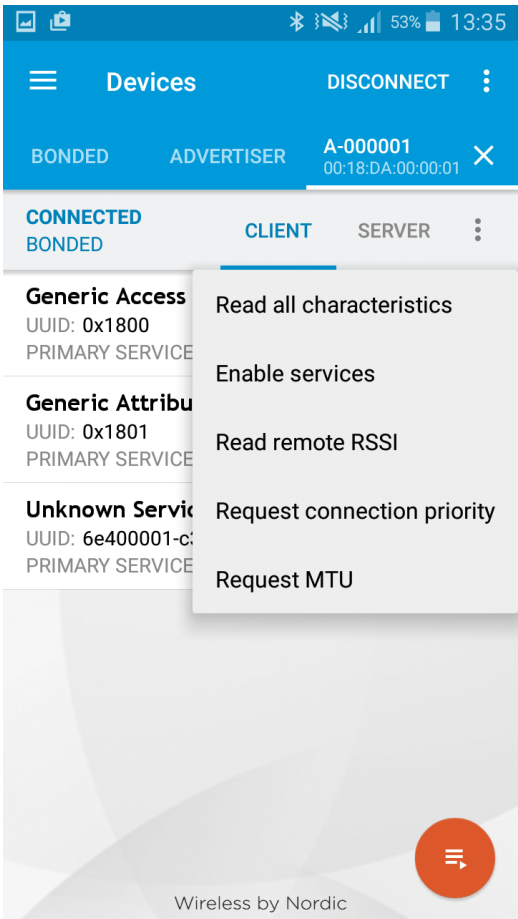
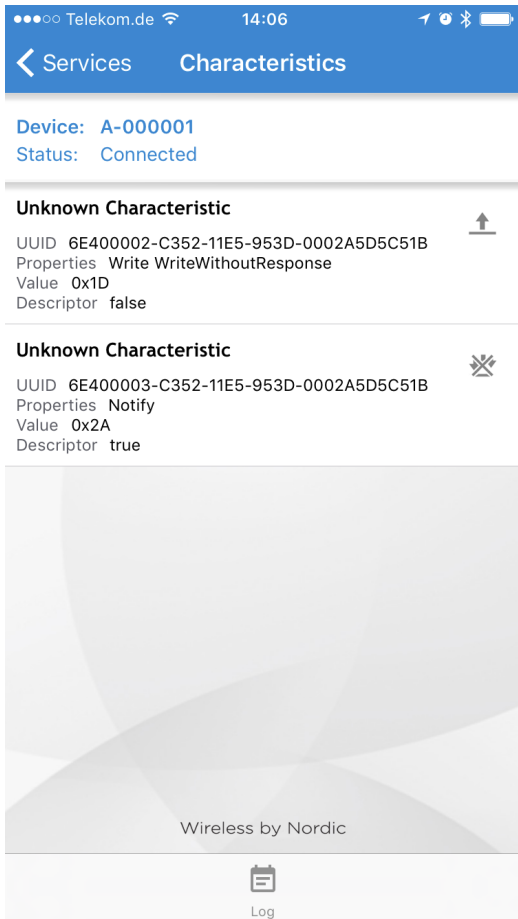
- Connect the module to a PC and open a terminal program using the Proteus default UART settings (115200 Baud, 8n1).
- Set the module into peripheral only mode as described in chapter 3.1. Initially, the module is advertising. Thus the Proteus *LED_1* is blinking.
- Start your smart phone, enable the Bluetooth® LE feature and start the nRF Connect App.
- Press "SCAN" to find the module on the radio.
- 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).

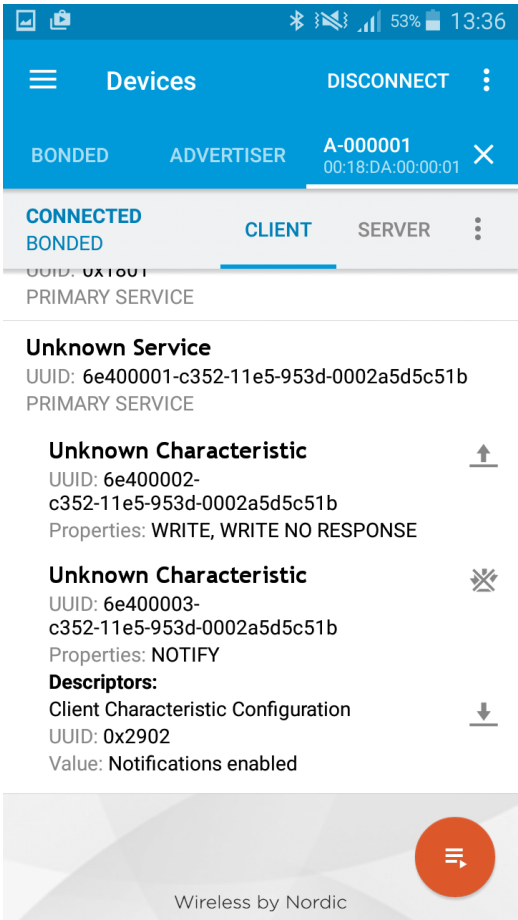
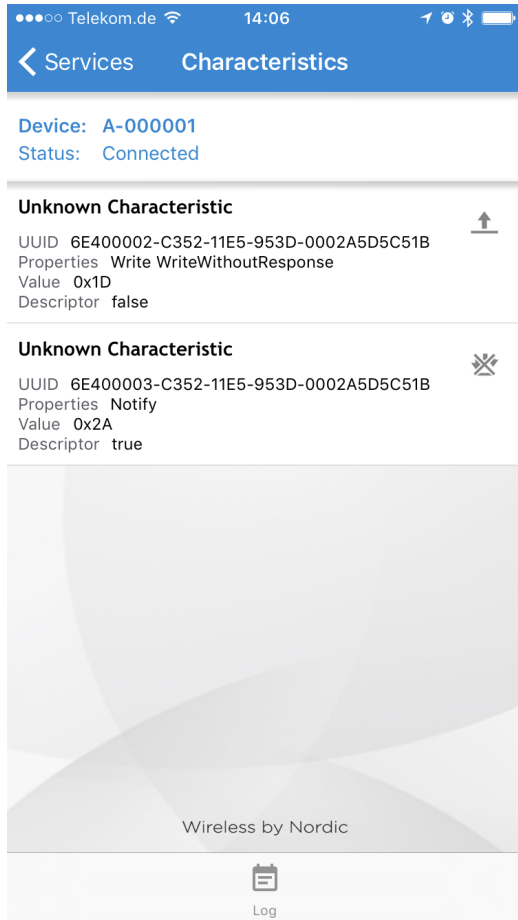


Android	iOS
<ul style="list-style-type: none"> • As soon as the module has received the connection request the module <i>LED_1</i> (<i>LED_3</i> on the Proteus-EV) will constantly light up. • Then the Proteus request for the static passkey. In default, the passkey is "123123". • The Bluetooth® coupling 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. 	
 <p>The image shows an Android smartphone screen with a Bluetooth pairing dialog box. The dialog is titled "Bluetooth-Kopplungsanforderung". It contains the text: "Zum Koppeln mit: A2621", "Geben Sie die PIN dieses Geräts ein:", and a hint "(Versuchen Sie 0000 oder 1234)". At the bottom of the dialog are two buttons: "ABBRECHEN" and "OK". Below the dialog is a numeric keypad with digits 1-9, 0, and an "OK" button.</p>	 <p>The image shows an iOS smartphone screen with a Bluetooth pairing dialog box. The dialog is titled "Kopplungsanforderung (Bluetooth)". It contains the text: "„A-000001“ möchte sich mit deinem iPhone koppeln. Gib den auf „A-000001“ gezeigten Code ein." Below the text is a text input field with a masked PIN ".....". At the bottom of the dialog are two buttons: "Abbrechen" and "Koppeln". Below the dialog is a numeric keypad with digits 1-9, 0, and a backspace button.</p>

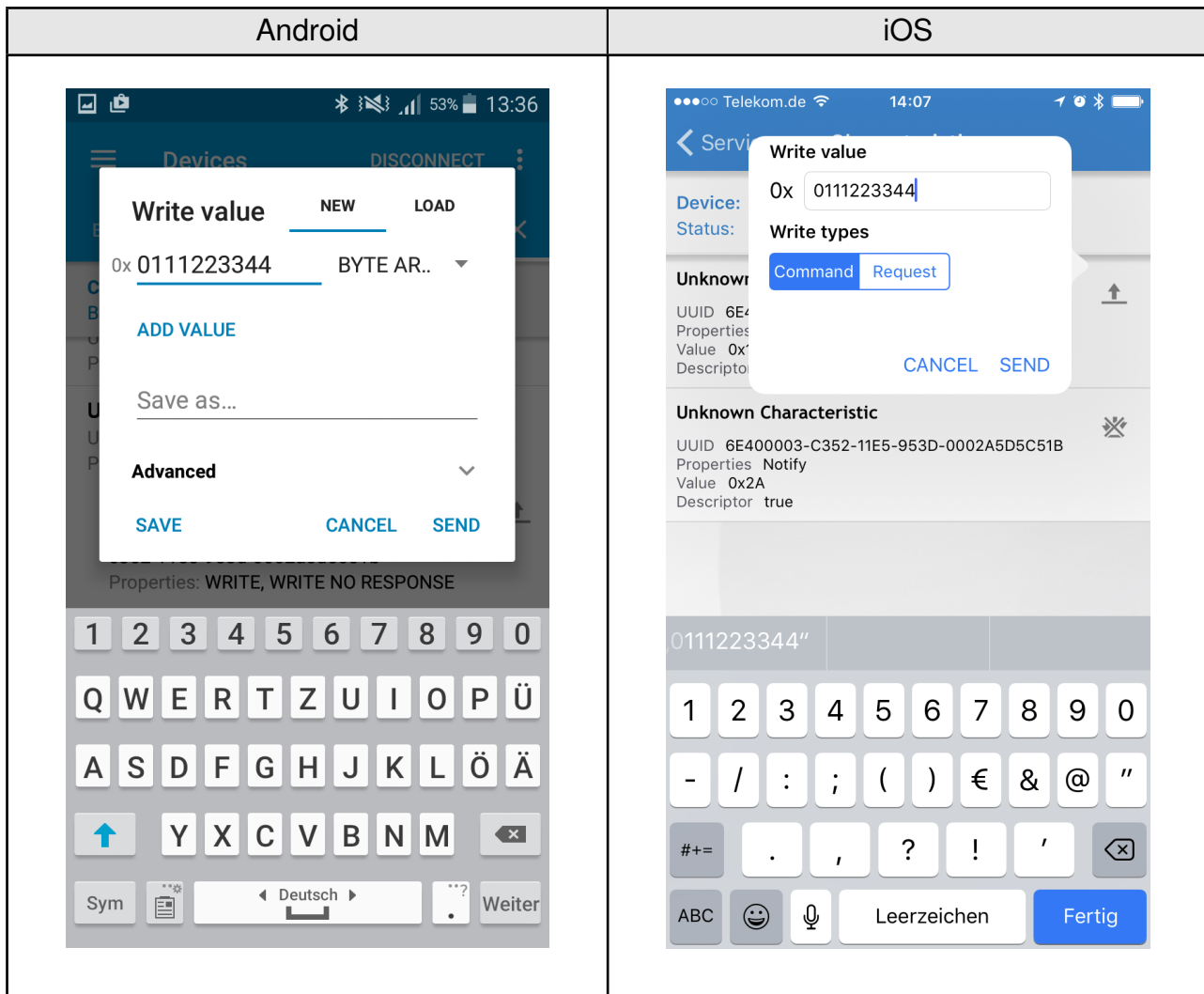
Android	iOS
<ul style="list-style-type: none"> • Now you are authenticated. • Please click on the menu bullets on the right and press "Request MTU" to request for a larger MTU. 	<ul style="list-style-type: none"> • Now you are authenticated. • Please click on the "Unknown Service" to start the service discovery and the MTU request. 

Android	iOS
<ul style="list-style-type: none"> The Proteus allows an MTU of up to 247 bytes, which results in a payload size of 243 bytes. 	<ul style="list-style-type: none"> The iOS App runs this step simultaneously in the background, a user-defined MTU is not possible.

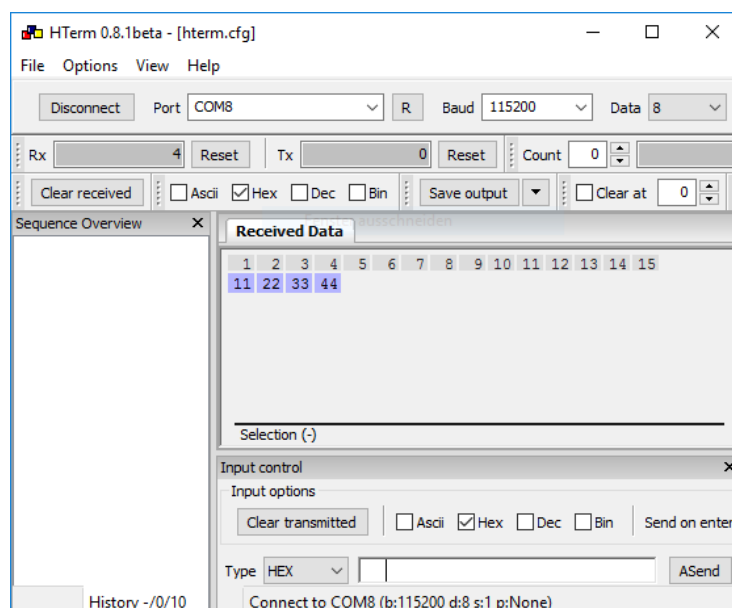
Android	iOS
<ul style="list-style-type: none"> Again click on the menu bullets on the right and press "Enable services" to enable the notifications. 	<ul style="list-style-type: none"> Press the arrows on the RX-characteristic 6E400003- C352-11E5- 953D -0002A5D5C51B to enable the notifications. Press 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. 
<ul style="list-style-type: none"> As soon as the module has received the notification enable request the Proteus <i>LED_2</i> (<i>LED_2</i> on the Proteus-EV) is turned on. 	

Android	iOS
	

- 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 selected 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. So unless you know for sure you have a higher MTU do not use a payload longer than 19 bytes.



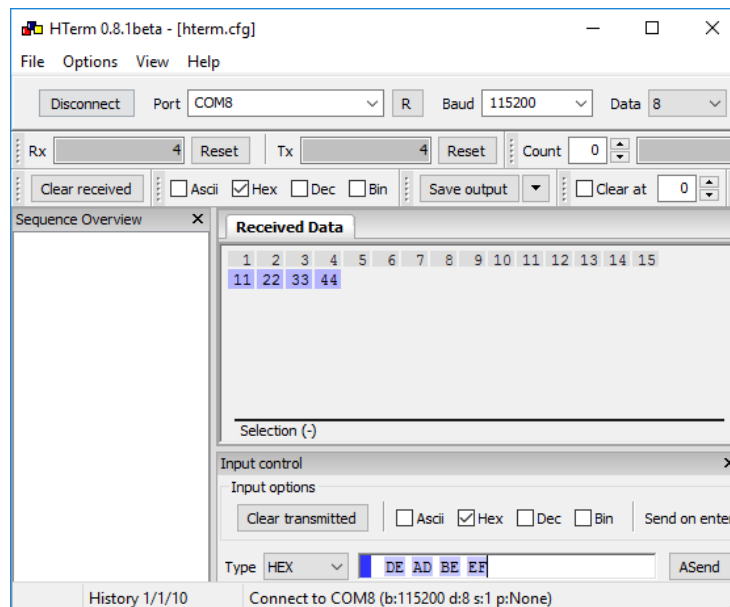
- The payload that has been sent is output by the Proteus via UART. In peripheral only mode, a transparent UART interface is used. This means, that only payload data is transmitted, without any packet header or footer. Thus the transmitted bytes 0x11 0x22 0x33 0x44 are displayed on the connected terminal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

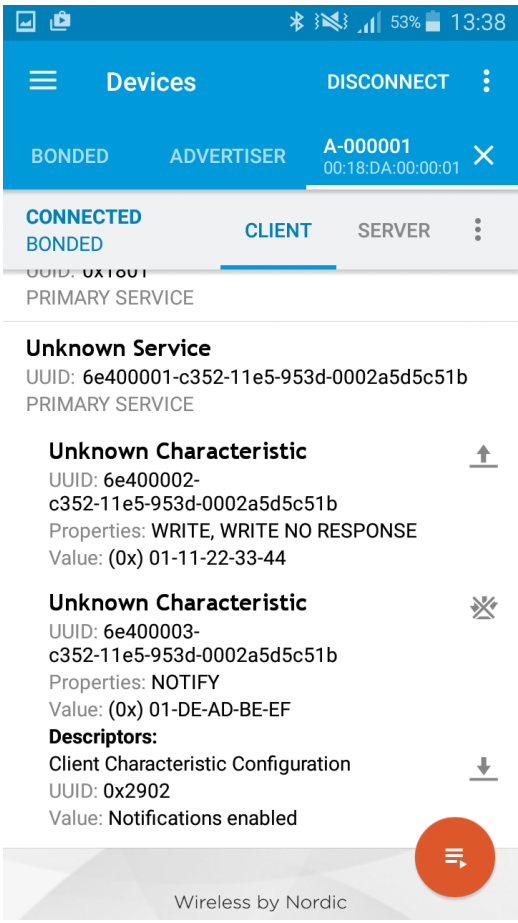
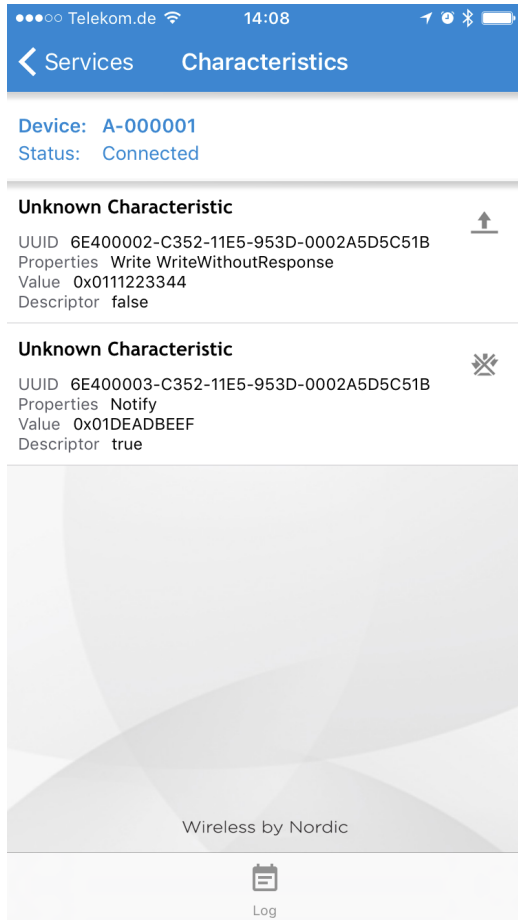


Android

iOS

- To send back data simply enter your payload (here we choose 0xDE 0xAD 0xBE 0xEF) in the respective terminal program field and press enter. The header 0x01 will be automatically applied by the module and is not to be transmitted by the host.
- The smallest supported MTU for all Bluetooth® 4.0 (or newer) devices result in a max payload of 19 bytes. So unless you know for sure you have a higher MTU do not use a payload longer than 19 bytes. All payload bytes outside the current supported channel payload are be discarded without notification to the host.



Android	iOS
<ul style="list-style-type: none"> 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. 	

4 Preconfiguring of the module

In case user settings (such as UART baud rate or static passkey) 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).



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



It is not recommended to change any other user-setting parameter than the two mentioned above.



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

5 Important notes

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

5.1 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.

5.2 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.

5.3 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.

5.4 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.

5.5 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 5.1 and 5.2 remains unaffected. All wireless connectivity module driver software "wireless connectivity SDK" and its source codes as well as all PC software tools are not subject to the Product Change Notification information process.

5.6 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.

5.7 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.

5.8 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.

6 Legal notice

6.1 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.

6.2 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 information 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. KG and its representatives against any damages arising out of the use of any Würth Elektronik eiSos GmbH & Co. KG components in safety-critical applications.

6.3 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.

6.4 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.

7 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.

7.1 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.

7.2 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.

7.3 Ownership

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

7.4 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.

7.5 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.

7.6 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.

7.7 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.

7.8 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.

7.9 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

1	Proteus-I evaluation board with USB cable	5
2	On Proteus-I and Proteus-II evaluation board, set these jumpers to start the peripheral only mode after reset.	7
3	On Proteus-III evaluation board, set these jumpers to start the peripheral only mode after reset.	7
4	Steps for the connection setup in static passkey mode (default)	9

List of Tables



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

