RE866 BT
Software User Guide

1VV0301530 Rev. 0 – 2018-05-03

TELIT
TECHNICAL
DOCUMENTATION

SPECIFICATIONS ARE SUBJECT TO CHANGE WITHOUT NOTICE

NOTICE

While reasonable efforts have been made to assure the accuracy of this document, Telit assumes no liability resulting from any inaccuracies or omissions in this document, or from use of the information obtained herein. The information in this document has been carefully checked and is believed to be reliable. However, no responsibility is assumed for inaccuracies or omissions. Telit reserves the right to make changes to any products described herein and reserves the right to revise this document and to make changes from time to time in content hereof with no obligation to notify any person of revisions or changes. Telit does not assume any liability arising out of the application or use of any product, software, or circuit described herein; neither does it convey license under its patent rights or the rights of others.

It is possible that this publication may contain references to, or information about Telit products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that Telit intends to announce such Telit products, programming, or services in your country.

COPYRIGHTS

This instruction manual and the Telit products described in this instruction manual may be, include or describe copyrighted Telit material, such as computer programs stored in semiconductor memories or other media. Laws in the Italy and other countries preserve for Telit and its licensors certain exclusive rights for copyrighted material, including the exclusive right to copy, reproduce in any form, distribute and make derivative works of the copyrighted material. Accordingly, any copyrighted material of Telit and its licensors contained herein or in the Telit products described in this instruction manual may not be copied, reproduced, distributed, merged or modified in any manner without the express written permission of Telit. Furthermore, the purchase of Telit products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents or patent applications of Telit, as arises by operation of law in the sale of a product.

COMPUTER SOFTWARE COPYRIGHTS

The Telit and 3rd Party supplied Software (SW) products described in this instruction manual may include copyrighted Telit and other 3rd Party supplied computer programs stored in semiconductor memories or other media. Laws in the Italy and other countries preserve for Telit and other 3rd Party supplied SW certain exclusive rights for copyrighted computer programs, including the exclusive right to copy or reproduce in any form the copyrighted computer program. Accordingly, any copyrighted Telit or other 3rd Party supplied SW computer programs contained in the Telit products described in this instruction manual may not be copied (reverse engineered) or reproduced in any manner without the express written permission of Telit or the 3rd Party SW supplier. Furthermore, the purchase of Telit products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents or patent applications of Telit or other 3rd Party supplied SW, except for the normal non-exclusive, royalty free license to use that arises by operation of law in the sale of a product.

USAGE AND DISCLOSURE RESTRICTIONS

I. License Agreements

The software described in this document is the property of Telit and its licensors. It is furnished by express license agreement only and may be used only in accordance with the terms of such an agreement.

II. Copyrighted Materials

Software and documentation are copyrighted materials. Making unauthorized copies is prohibited by law. No part of the software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without prior written permission of Telit.

III. High Risk Materials

Components, units, or third-party products used in the product described herein are NOT fault-tolerant and are NOT designed, manufactured, or intended for use as on-line control equipment in the following hazardous environments requiring fail-safe controls: the operation of Nuclear Facilities, Aircraft Navigation or Aircraft Communication Systems, Air Traffic Control, Life Support, or Weapons Systems (High Risk Activities"). Telit and its supplier(s) specifically disclaim any expressed or implied warranty of fitness for such High Risk Activities.

IV. Trademarks

TELIT and the Stylized T Logo are registered in Trademark Office. All other product or service names are the property of their respective owners.

V. Third Party Rights

The software may include Third Party Right software. In this case you agree to comply with all terms and conditions imposed on you in respect of such separate software. In addition to Third Party Terms, the disclaimer of warranty and limitation of liability provisions in this License shall apply to the Third Party Right software.

TELIT HEREBY DISCLAIMS ANY AND ALL WARRANTIES EXPRESS OR IMPLIED FROM ANY THIRD PARTIES REGARDING ANY SEPARATE FILES, ANY THIRD PARTY MATERIALS INCLUDED IN THE SOFTWARE, ANY THIRD PARTY MATERIALS FROM WHICH THE SOFTWARE IS DERIVED (COLLECTIVELY “OTHER CODE”), AND THE USE OF ANY OR ALL THE OTHER CODE IN CONNECTION WITH THE SOFTWARE, INCLUDING (WITHOUT LIMITATION) ANY WARRANTIES OF SATISFACTORY QUALITY OR FITNESS FOR A PARTICULAR PURPOSE.

NO THIRD PARTY LICENSORS OF OTHER CODE SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND WHETHER MADE UNDER CONTRACT, TORT OR OTHER LEGAL THEORY, ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE OTHER CODE OR THE EXERCISE OF ANY RIGHTS GRANTED UNDER EITHER OR BOTH THIS LICENSE AND THE LEGAL TERMS APPLICABLE TO ANY SEPARATE FILES, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

APPLICABILITY TABLE

PRODUCTS

- RE866A1-EU
- RE866A1-NA

CONTENTS

1. INTRODUCTION

1.1. Scope

This document describes the usage of the Bluetooth module RE866.

1.2. Audience

This document is intended for Telit customers, especially system integrators, about to implement Bluetooth modules in their application.

1.3. Contact and Support Information

For general contact, technical support services, technical questions and report documentation errors contact Telit Technical Support at:

- TS-SRD@telit.com

Alternatively, use:

https://www.telit.com/contact-us

For detailed information about where you can buy Telit modules or for recommendations on accessories and components visit:

https://www.telit.com

Our aim is to make this guide as helpful as possible. Keep us informed of your comments and suggestions for improvements.

Telit appreciates feedback from the users of our information.

1.4. Text Conventions

Danger – This information MUST be followed or catastrophic equipment failure or bodily injury may occur.

Caution or Warning – Alerts the user to important points about integrating the module, if these points are not followed, the module and end user equipment may fail or malfunction.

Tip or Information – Provides advice and suggestions that may be useful when integrating the module.

All dates are in ISO 8601 format, i.e. YYYY-MM-DD.

1.5. Related Documents

- [1] RE866 Hardware User Guide, 1VV0301364 (EU), 1VV0301525 (NA)
- [2] RE866 AT Command Reference, 80555ST10865A
- [3] Bluetooth 5.0 Core Specification
- [4] UICP+ UART Interface Control Protocol, 30507ST10756A

2. FEATURE SET

The combined central and peripheral RE866 firmware includes the following feature set:

- Terminal I/O in central and peripheral role
- Fix pin for easy security
- AT command mode
- Advanced power saving features like UICP and SYSTEMOFF
- Firmware update via Bluetooth
- Bluetooth LE secure connections
- NFC Handover

This document shows the practical use of some AT commands listed in the AT command reference. For command details please refer to the *RE866 AT Command Reference*.

3. BLUETOOTH

3.1. Modes and Connections

In AT command mode the RE866 supports one central or one peripheral Terminal I/O connection. This means that the RE866 stops advertising (being connectable) as soon as a central or peripheral connection is established.

When a peripheral Terminal I/O server connection is active, it is not possible to establish a central connection to be used as Terminal I/O client.

The reason for this behavior is that a Terminal I/O connection in AT mode puts the serial interface in data mode, where it is not possible to handle AT commands or events for an additional central connection. Therefore, it is not possible to use the ATD command for connection establishment during a Terminal I/O connection.

3.2. AT Command Mode

This chapter describes connection examples for different roles:

- Central role: TIO connections to BLE TIO peripheral devices in AT command mode
- Peripheral role as Terminal I/O server

3.2.1. Central Role as Terminal I/O central

In central role the RE866 supports the possibility to connect to Terminal I/O peripheral devices only.

3.2.1.1. Searching for Available Peripheral Devices

If the Bluetooth address of the TIO peripheral device is unknown the RE866 needs to scan for available peripheral devices first.

AT+LESCAN	00802554F6AA,t2 RSSI:-77 TYPE:CONN NAME:BM+S42 6AA MNF:8F0009B0011000 UUID:FEFB 008025598B2D,t2 RSSI:-53 TYPE:CONN NAME:BM+S42 B2D MNF:8F0009B0011000 UUID:FEFB 00802554F77A,t2 RSSI:-82 TYPE:CONN NAME:BM+S50 77A MNF:8F0009B0011000 UUID:FEFB 008025D1D434,t2 RSSI:-86 TYPE:CONN NAME:BM+S42M/SRV D434 MNF:8F0009B0011000 UUID:FEFB 0080254800FC,t2 RSSI:-89 TYPE:CONN NAME:BM+SR 00FC MNF:8F0009B0011000 UUID:FEFB OK

Example: This output lists 5 different TIO peripheral devices.

3.2.1.2. Connect to a Terminal I/O device

ATD00802554F6AA,TIO	CONNECT TIO 0x10

3.2.1.3. Close Terminal I/O Connection

The Terminal I/O connection can be closed by using the AT command ATH.

Using the ATH command example:

<wait 1 sec after data exchange> +++ ATH=0x01	 OK NO CARRIER 0x10

The response of the disconnect request reports the event “NO CARRIER” followed by disconnected connection handle.

The same event is reported when the remote Terminal I/O client side disconnects the connection.

3.2.2. Peripheral Role as Terminal I/O Server

A Terminal I/O connection to the RE866 can be created from each Bluetooth Low Energy device that supports the Terminal I/O client role.

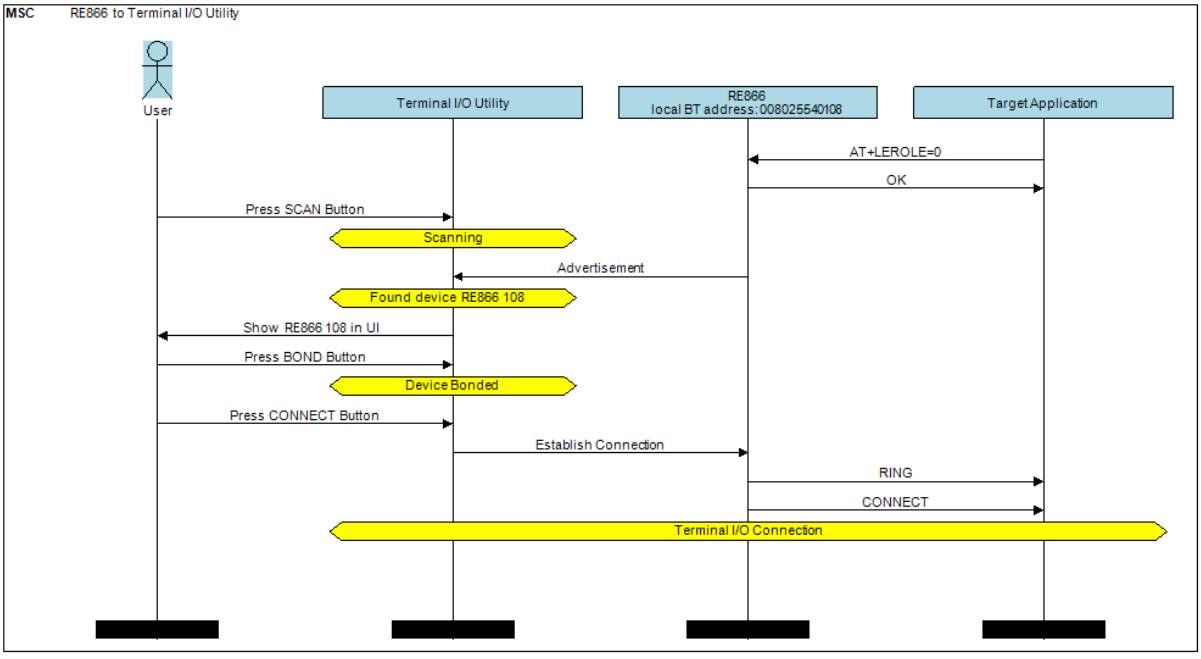
Telit provide the Terminal I/O client implementation for iOS and Android.

To establish a Bluetooth Low Energy connection from a smartphone to the RE866 the "Terminal IO Utility" app from Telit needs to be installed on the smartphone.

The following QR-Codes provide the link to download the "Terminal IO Utility" app.

iOS **Logo** **Android**

The Terminal IO Utility app allows the user to connect to Terminal I/O peripheral devices (RE866) and exchange data providing a simple terminal emulation.



As soon as the connection is established data can be sent from the smartphone to RE866 and vice versa.

3.2.2.1. Incoming Terminal I/O Connection

For a Terminal I/O connection it is necessary that the Terminal I/O service and the advertising mode are enabled. This is the default behavior of the RE866.

The RE866 signals an incoming Terminal I/O connection with the following event.

	RING CONNECT TIO 0x01

The RE866 reports the incoming Terminal I/O connection with the result message “RING”. The established Terminal I/O connection is reported with the message ”CONNECT“ including the connection type “TIO“ and a connection handle “0x01”.

The given connection handle is required for detailed activities onto this Terminal I/O connection.

After reporting the “CONNECT” result message the RE866 changed from the AT based “command mode” to the “online data mode”.

3.2.2.2. Exchange Terminal I/O Data

All data send on the serial interface are transparently sent to the Terminal I/O client side.

All data send by the remote Terminal I/O client are binary output on the serial interface of the RE866.

3.2.2.3. Close Terminal I/O Connection

The Terminal I/O connection can be closed by using the AT command ATH.

Using the ATH command:

<wait 1 sec after data exchange> +++ ATH=0x01	 OK NO CARRIER 0x01

The response of the disconnect request reports the event “NO CARRIER” followed by disconnected connection handle.

The same event is reported when the remote Terminal I/O client side disconnects the connection.

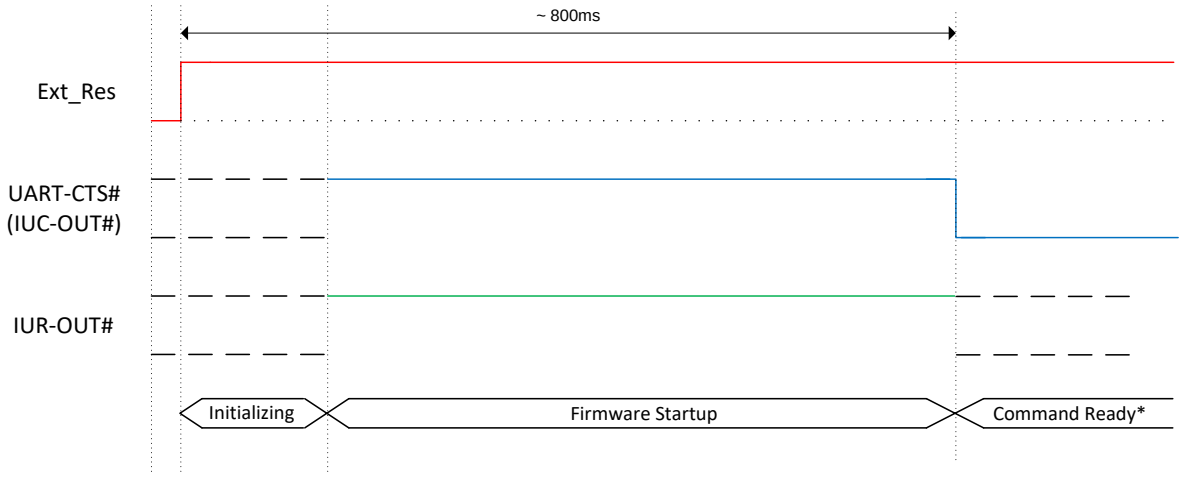
3.3. Startup Timing

The startup time until the RE866 is able to accept link requests or serial data depends on:

- The firmware version
- The usage of the UART Interface Control Protocol (UICP)

For more details about the UICP protocol please refer to the document *UICP+ UART Interface Control Protocol [4]*.

The following diagram shows the startup timing of the RE866 based on firmware version 1.1 and UICP deactivated.



(*) The firmware is command ready ~800ms after the reset has been released and when UART-CTS# is low.

3.4. Security

This chapter describes the security mechanisms of the RE866 to control the access to the local Bluetooth devices characteristics. The pairing process is triggered automatically when an access to a characteristic is requested that requires security.

3.4.1. Pairable and Bondable Mode

In general, we distinguish between pairing and bond. Pairing is the active process to generate a set of encryption keys. The paring can be done with or without user interaction depending of the I/O capabilities. The pairing will result in a bond if the generated data is stored in the bonded device list (AT+BNDLIST).

AT+BPAIRMODE controls if a pairing is performed or not.

Value	Description
0	No pairing allowed, RE866 advertises TIO as “functional”
1	Pairing allowed, RE866 advertises TIO as “bondable and functional” **(default)**

AT+BNDS controls the storing of the pairing information as bond.

Value	Description
0	Bonds persists for the duration of the authenticated connection
1	Bonds are permanently stored in the NVRAM of the RE866 **(default)**

The bonded device list is affected by the following commands:

- AT+BNDLIST shows the devices stored in the bonded device list
- AT+BNDSIZE determines the size of the bonded device list and deletes the whole list when decreasing the size below the number of currently bonded devices.
- AT+BNDS deletes the bonded device list
- AT+BNDDEL deletes single entries or the whole list
- AT&F1 deletes the bonded device list

If the bonded device list is full and another device is bonded, the least recently bonded device will be overwritten by the new one. If bonds are not required please set AT+BNDS=0.

3.4.2. LE Secure Connections

Since Bluetooth 4.2 a security mechanism called “Secure Connections” is supported.

LE Secure Connection introduces a method to generate a shared secret (key) in a way that ensures the data integrity and privacy of a connection even in cases where the pairing/bonding procedure was completely tapped with a Bluetooth sniffer if that shared secret is used for authentication and encryption.

Secure connection key generation is applicable for all authentication methods (e.g. just works or passkey entry) while all authentication trigged I/O activity remain the same as for legacy LE security but one new method (display yes/no) is introduced.

Since Bluetooth 4.2 it is mandated that LE Secure Connection key generation is used while pairing/bonding if both devices of a given connection support this feature. If one device of a

given connection only supports LE legacy security key generation procedures these legacy procedures will be used instead.

From user point of view this negotiation is mostly transparent and backward compatible. The only exceptions are if LE Secure Connection is mandated (AT+LETIO=4) or the new display yes/no (AT+BIOCAP=1) configuration is used.

By configuring AT+LETIO=4 for incoming Terminal I/O connections LE Secure Connection usage is mandated for incoming Terminal I/O connections. In such case Terminal I/O connections from devices that only support LE legacy security are rejected.

By configuring AT+BIOCAP=1 for I/O capabilities “display yes/no”, the “yes/no” functionality is only used for LE Secure Connection procedures.

For LE legacy security, only the “display” functionality is used so the results are the same as for a “display only” configuration.

3.4.3. Security Levels for Terminal I/O

The behavior of LE Security is configurable using the parameters for I/O capabilities (AT+BIOCAP) and a man in the middle protection (AT+BMITM).

The security level of Terminal I/O is configurable using the parameter AT+LETIO.

Value	Description
0	Terminal I/O service disabled (no advertising, no characteristics)
1	Terminal I/O service enabled, security is required with encryption (no MITM)
2	Terminal I/O service enabled, no security (authentication or encryption) required **(default)**
3	Terminal I/O service enabled, authenticated pairing with encryption (MITM required)
4	Terminal I/O service enabled, authenticated LE secure connections pairing with encryption (MITM required, LE secure connections required)

AT+BIOCAP sets the input and output capabilities of the device used for LE Security.

Value	Description
0	Display only
1	Display Yes/No
2	Keyboard only
3	No input no output **(default)**
4	Display and keyboard

AT+BMITM controls the man in the middle (MITM) protection of the device during LE Security.

Value	Description
0	Parameter disabled, connection and service based configuration applies (see **ATD** command and **AT+LETIO** parameter) **(default)**
1	Man in the middle protection enabled (connection and service based configuration is ignored)

LE Security defines the following association models based on the Input/Output (I/O) capabilities of the two devices:

- **Just Works**

This method is used when at least one of the devices does not have display capability of six digits and is not capable of entering six decimal digits using a keyboard or any other means (no I/O).

This method does not provide MITM protection (see 3.4.4 Connection Example Terminal I/O “Just Works”).

- **Passkey Entry**

This method may be used between a device with a display and a device with numeric keypad entry (such as a keyboard), or two devices with numeric keypad entry (see 3.4.5 Connection Example Terminal I/O “Passkey Entry”).

In the first case, the display is used to show a six digit numeric code to the user, who then enters the code on the keypad.

In the second case, the user of each device enters the same six digit numeric code.

Both cases provide MITM protection.

Possible combinations of I/O capabilities and the possibility of MITM protection are listed in the table below. For each case of the “MITM protection” an example of the serial messages between the RE866 and the DTE are listed.

In case the user chooses a scenario where MITM protection is not allowed but one of the communication devices is configured to MITM protection, the pairing is refused.

- **Numeric Comparison**

This method may be used between two devices with a display and keys that allow the user to accept or reject a connection.

If the “Display Yes/No” or “Display and keyboard” capability is supported by both devices the displays show a 6 digit numerical code. The user is then requested to compare the codes of both displays. If the codes on both displays are equal the user can accept the connection by pressing the “yes” input of both devices. In case the user presses the “no” input on at least one of the devices the pairing becomes rejected.

This method provides MITM protection.

Responder / Initiator	Display only	Display Yes/No	Keyboard only	No input no output	Display and keyboard
Display only AT+BIOCAP=0	Just Works (both automatic confirmation) *No MITM protection*	Just Works (both automatic confirmation) *No MITM protection*	Passkey entry (initiator displays, responder inputs) *MITM protection* SSPPIN <BT addr> <passkey>	Just Works (both automatic confirmation) *No MITM protection*	Passkey entry (initiator displays, responder inputs) *MITM protection* SSPPIN <BT addr> <passkey>
Display Yes/No AT+BIOCAP=1	Just Works (both automatic confirmation) *No MITM protection*	Just Works (for LE legacy pairing) (both automatic confirmation) *No MITM protection* --- Numeric comparison (for LE secure connections) *MITM protection* SSPCONF <BT addr> <passkey> ? AT+BSSPCONF <BT addr>,1	Passkey entry (initiator displays, responder inputs) *MITM protection* SSPPIN <BT addr> <passkey>	Just Works (both automatic confirmation) *No MITM protection*	Passkey entry (for LE legacy pairing) (initiator displays, responder inputs) *MITM protection* SSPPIN <BT addr> <passkey> --- Numeric comparison (for LE secure connections) *MITM protection* SSPCONF <BT addr> <passkey> ? AT+BSSPCONF <BT addr>,1
Keyboard only AT+BIOCAP=2	Passkey entry (responder displays, initiator inputs) *MITM protection* SSPPIN <BT addr> ? AT+BSSPPIN <BT addr>,<passkey>	Passkey entry (responder displays, initiator inputs) *MITM protection* SSPPIN <BT addr> ? AT+BSSPPIN <BT addr>,<passkey>	Passkey entry (initiator and responder inputs) *MITM protection* SSPPIN <BT addr> ? AT+BSSPPIN <BT addr>,<passkey>	Just Works (both automatic confirmation) *No MITM protection*	Passkey entry (responder displays, initiator inputs) *MITM protection* SSPPIN <BT addr> ? AT+BSSPPIN <BT addr>,<passkey>
No input no output AT+BIOCAP=3	Just Works (both automatic confirmation) *No MITM protection*	Just Works (both automatic confirmation) *No MITM protection*	Just Works (both automatic confirmation) *No MITM protection*	Just Works (both automatic confirmation) *No MITM protection*	Just Works (both automatic confirmation) *No MITM protection*
Display and keyboard AT+BIOCAP=4	Passkey entry (responder displays, initiator inputs) *MITM protection* SSPPIN <BT addr> ? AT+BSSPPIN <BT addr>,<passkey>	Passkey entry (for LE legacy pairing) (responder displays, initiator inputs) *MITM protection* SSPPIN <BT addr> ? AT+BSSPPIN <BT addr>,<passkey> --- Numeric comparison (for LE secure connections) *MITM protection* SSPCONF <BT addr> <passkey> ? AT+BSSPCONF <BT addr>,1	Passkey entry (initiator displays, responder inputs) *MITM protection* SSPPIN <BT addr> <passkey>	Just Works (both automatic confirmation) *No MITM protection*	Passkey entry (for LE legacy pairing) (initiator displays, responder inputs) *MITM protection* SSPPIN <BT addr> <passkey>SSPPIN <BT addr> <passkey> --- Numeric comparison (for LE secure connections) *MITM protection* SSPCONF <BT addr> <passkey> ? AT+BSSPCONF <BT addr>,1

Green color: RE866 output message SSPPIN <BT addr> ? (example)
Blue color: RE866 input request AT+BSSPPIN <BT addr> <passkey> (example)

The following flow charts will give an example for the different SSP authentication methods “just works” and “passkey entry” within an incoming call request from a smartphone (iOS or Android) using Telit’s Terminal I/O Utility app in combination with the RE866 (see also the connection example in chapter 3.2.2 Peripheral Role as Terminal I/O Server).

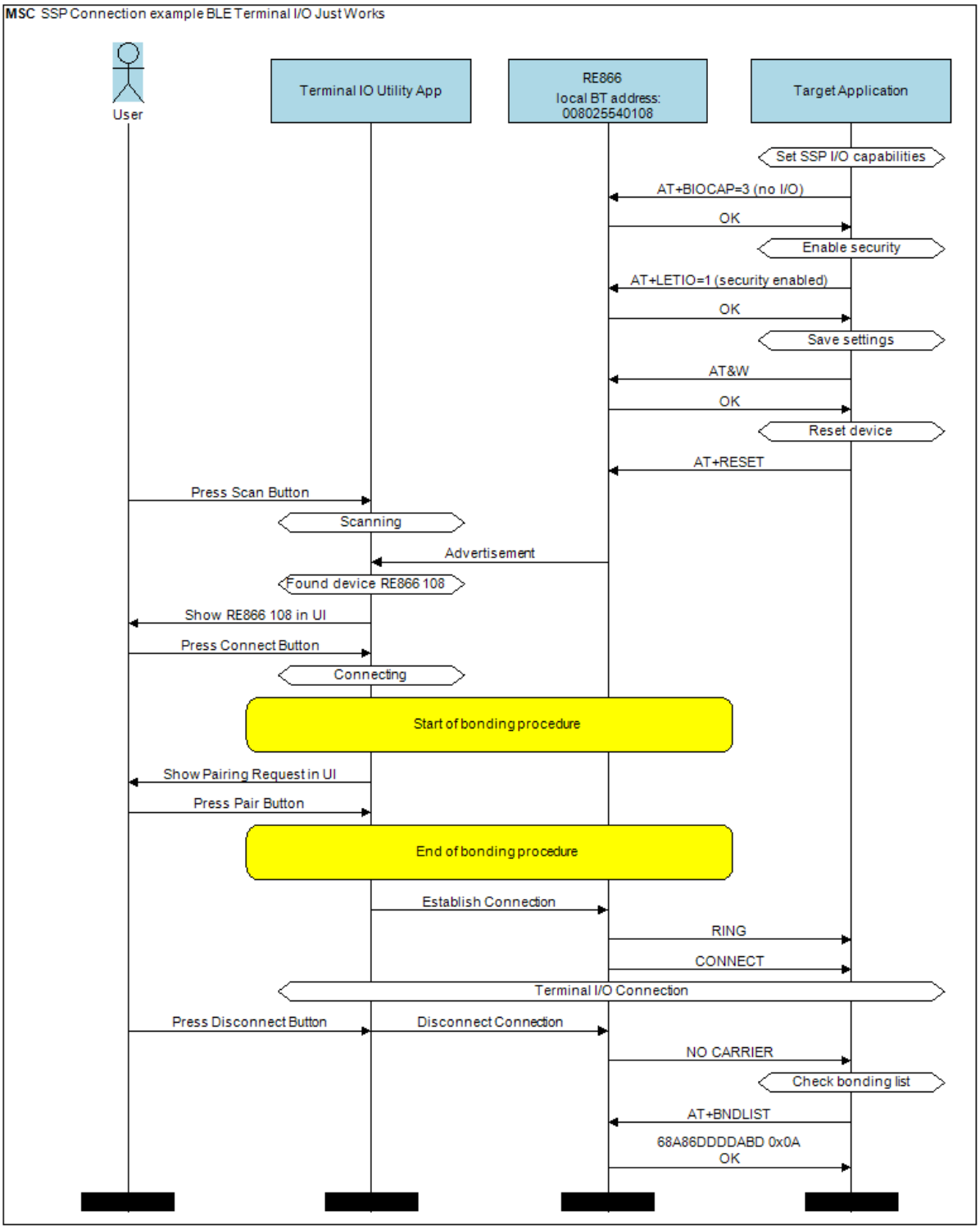
The “*Target Application*” part will simulate the device at the end (DTE) which communicates to the RE866 with configuration commands.

The interesting part of the bonding procedure is placed between the yellow boxes “*Start of bonding procedure*” and “*End of bonding procedure*”.

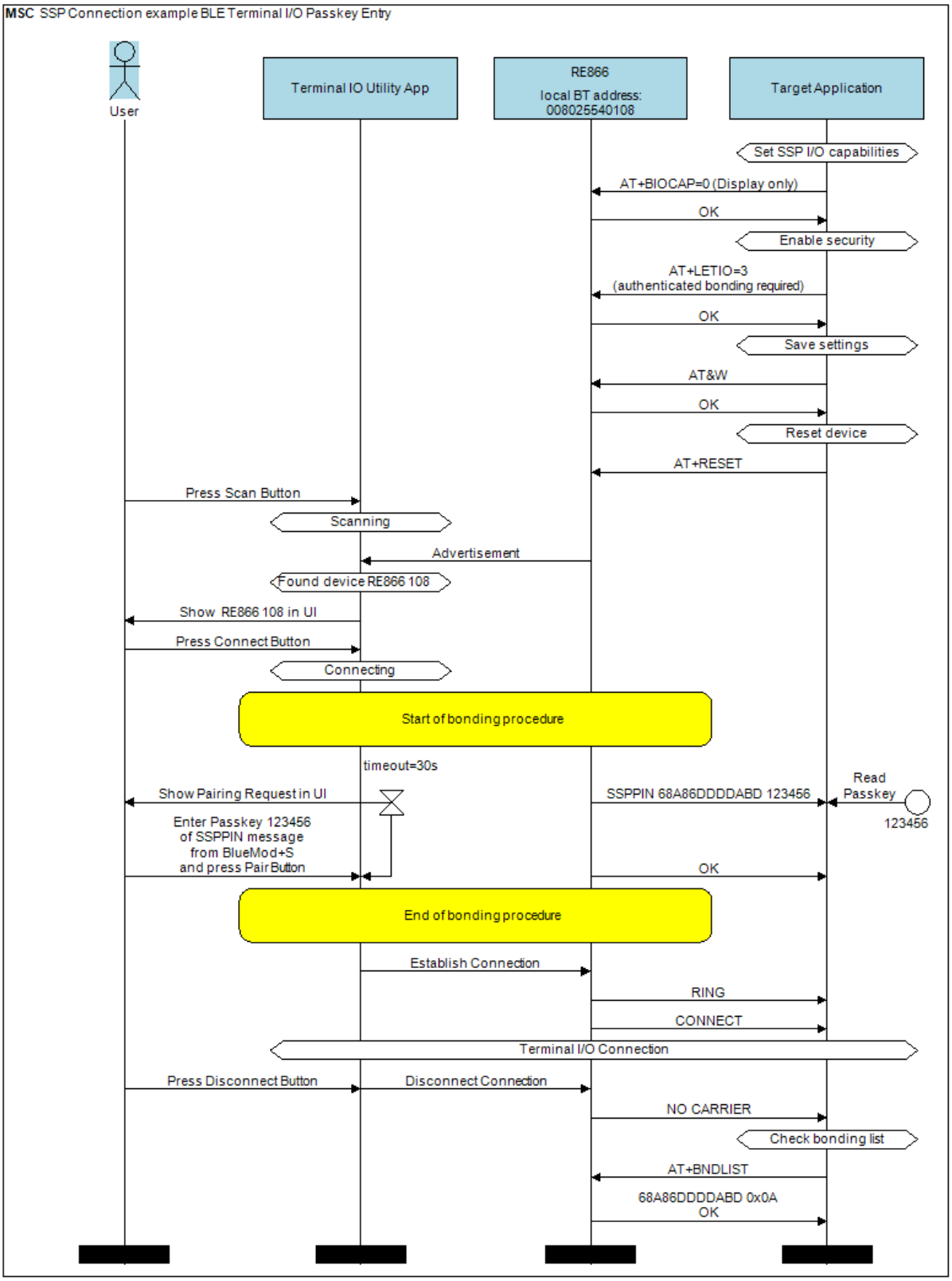
All serial commands between the “*Target Application*” and the “*RE866*” outside of the bonding procedure are used for preparation of LE Security configuration.

These configuration commands and responses within the flow charts are described in the *RE866 AT Command Reference [2]*.

3.4.4. Connection Example Terminal I/O “Just Works”



3.4.5. Connection Example Terminal I/O “Passkey Entry” with I/O capabilities “display only”



3.5. NFC Handover

The NFC functionality in the RE866 can be used to initiate a Bluetooth pairing procedure. NFC “reader/writer” option is not supported by the firmware.

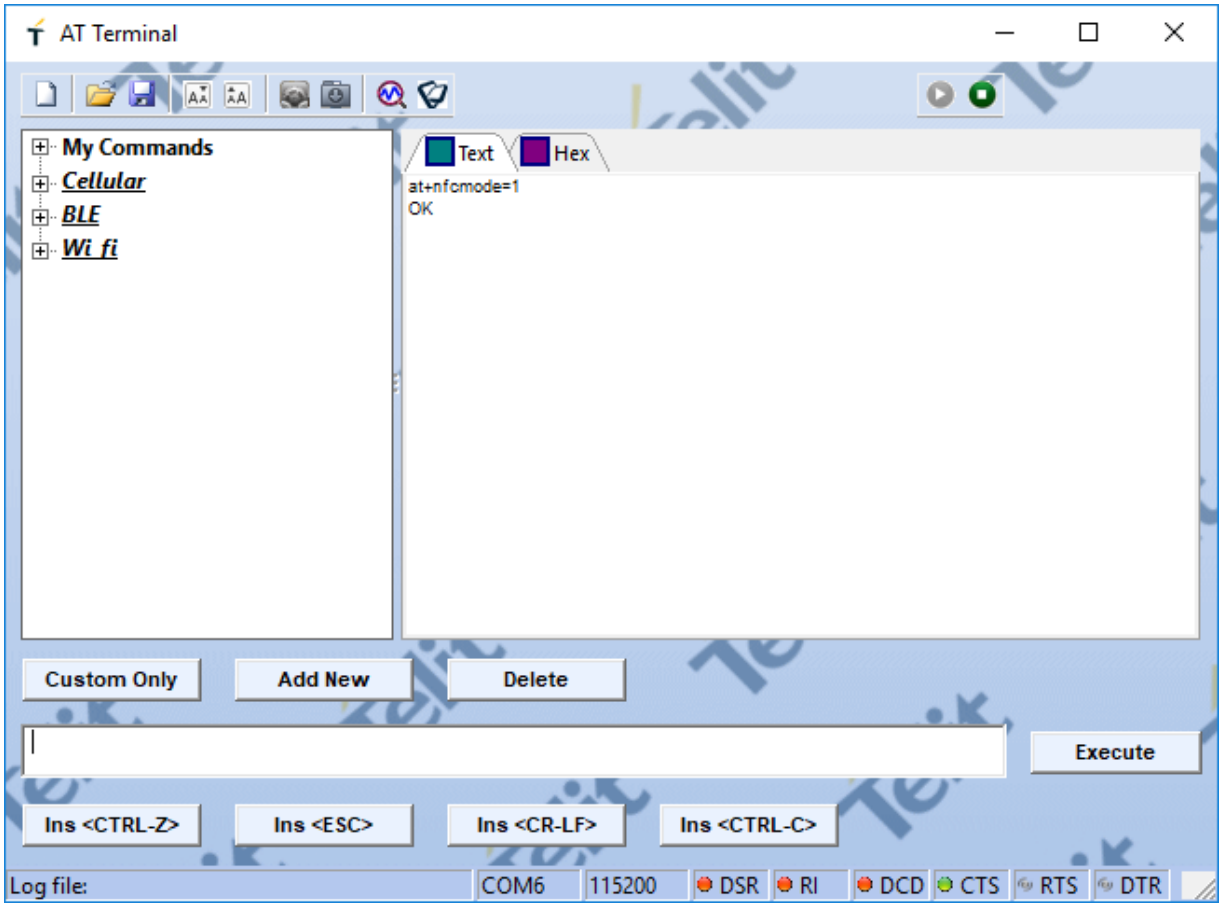
The NFC mode can be activated or deactivated by using the following AT command:

Syntax: AT+NFCMODE=<value>

Value	Description
0	NFC interface off **(default)**
1	Automatic mode

Enable the NFC Handover functionality by using the following AT command.

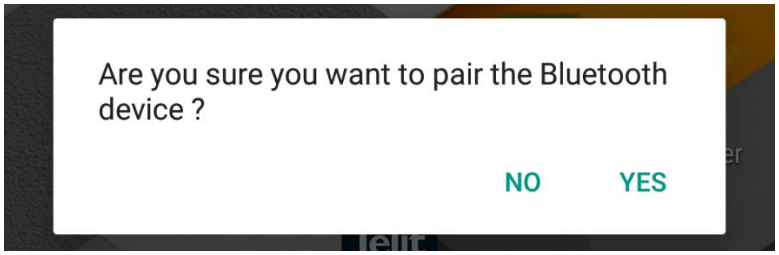
(optional: followed by AT&W to store the AT command permanently)



3.5.1. NFC Handover Example

Make sure NFC is available and enabled in the smartphone and move it over the NFC antenna.

The Bluetooth address will be read out and the smartphone initiates a Bluetooth pairing request to the device of the given Bluetooth address and a Bluetooth pairing request message will appear. Now continue with “Pair” or “Yes” to accept the Bluetooth pairing request scenario.



After the pairing request ended successfully you will find the new paired device within the Bluetooth settings of your smartphone.

4. LORA

4.1. Configure Network Server (MultiTech Conduit gateway)

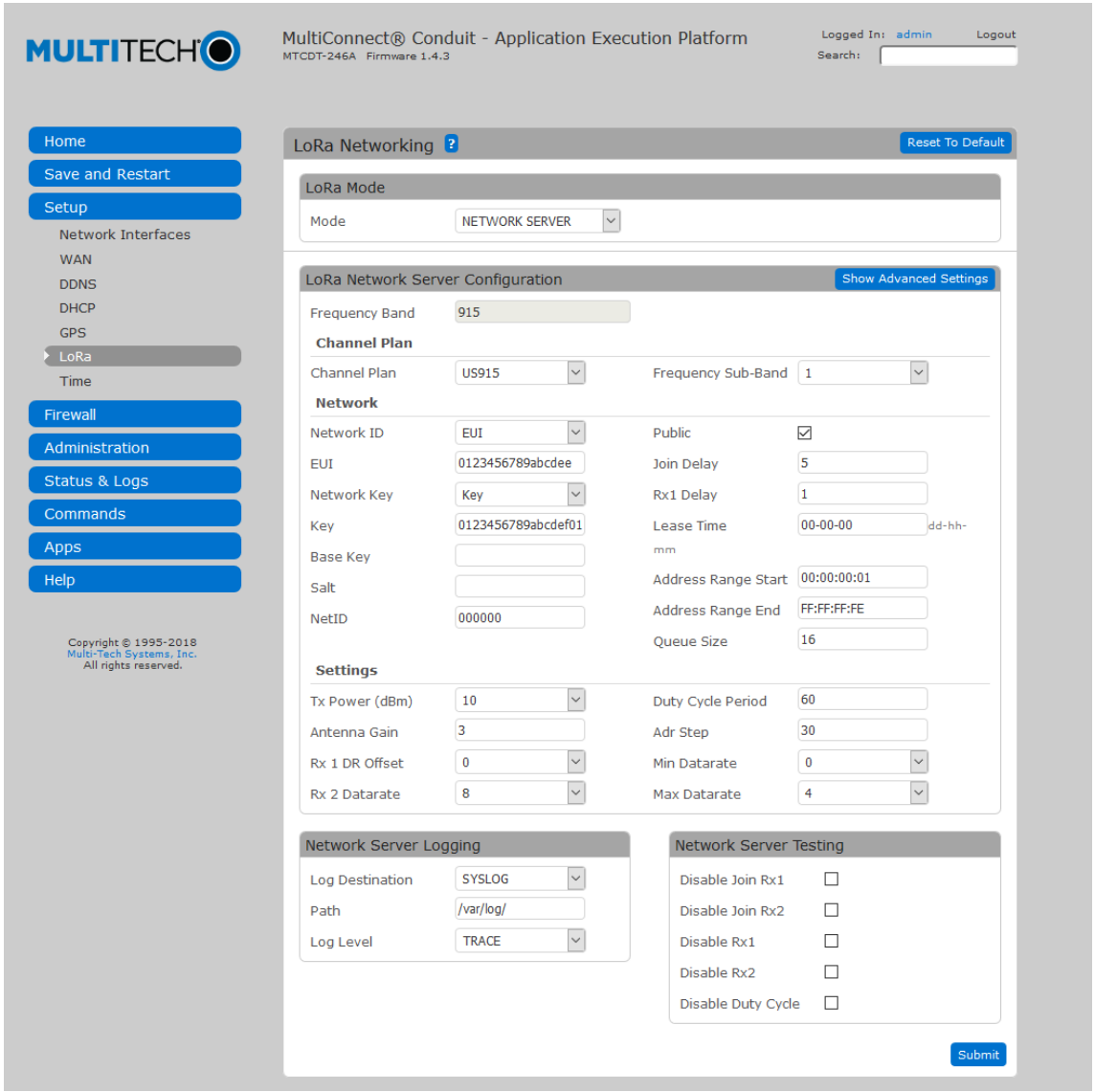
For the purposes of this guide, we assume that you have completed the initial hardware setup of the MultiTech Conduit gateway, the required LoRa mCard and the Ethernet connection as explained by MultiTech in their supporting materials.

When this is complete, you must configure the MultiTech gateway network server as follows: Log in to the LoRa Network Server Configuration panel (Setup > LoRa network server).

Configure the server by doing the following example:

Tick Public.
Set the Network EUI to **0123456789abcdee**.
Set the Network Key dropdown to **Key**.
Set the Key text field to **0123456789abcdef0123456789abcdef**.

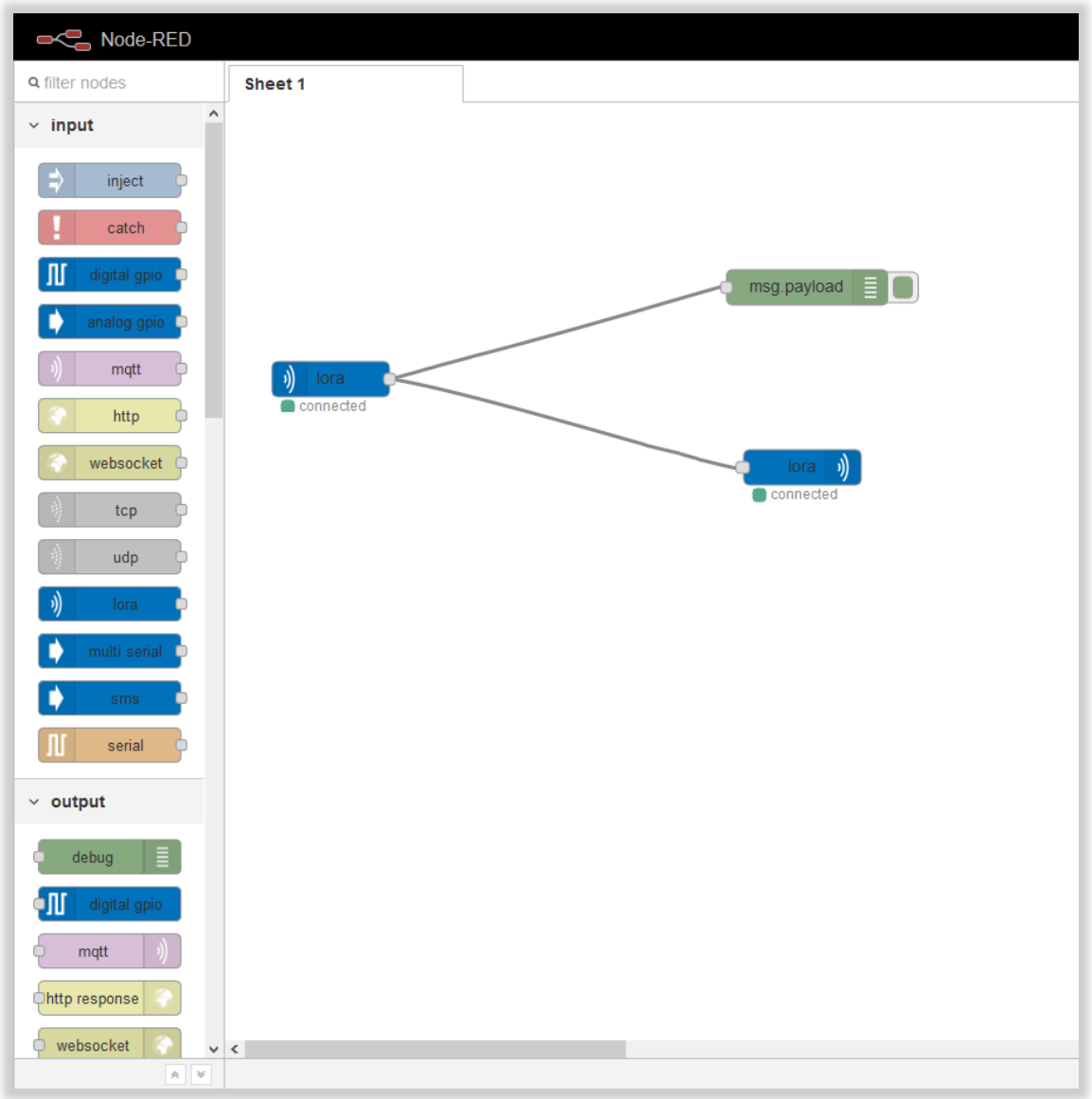
These settings are illustrated in the next figure (example: NA firmware) for the 915Mhz.



4.2. Configure Application

After the previous configuration you have to set up the application server using Node-RED.

Select Apps in the left menu to launch the Node-RED application. Configure Node-RED to send the message payload to the debug window and also to echo the payload back to the end device. The following image shows these settings configured in Node-RED.



4.3. Configure RE866

Now that the gateway has been configured we are ready to configure the RE866.

Power ON the module and check that the RE866 is accessible via UART (virtual COM port).

Open the COM port with a terminal program with 115200 bps, 8N1 and HW flow control activate.

Once you have established the UART connection successfully then you must set the same parameter as we used to configure the gateway.

The following AT commands refers to the previously configured gateway (see chapter 4.1).

Network ID is the AppEUI that you can set with the following AT command.

AT+LAPPEUI=0123456789abcdee	OK

The network key is the AppKey that you can set with the following command.

AT+LAPPKEY=0123456789abcdef0123456789abcdef	OK

After that we need to set the activation as OTAA with the following command.

AT+LJOINM=1	OK

We are ready now to join the network but before it, let's disable the BT advertising with the command.

AT+LEADE=3	OK

Now let's join the network.

AT+LJOINNET	OK DL,JOIN_SUCCESS

As shown if success you will get JOIN SUCCESS message otherwise JOIN FAIL or timeout.

Now we can send data with.

AT+LSENDDATA=1234,1	OK DL,ACK

In case you will send data from the gateway to the node you can have also.

AT+LSENDDATA=1234,1	OK DL,ACK,DATA

Where you can see also the DATA indication that mean that the server send data to the module and you can read with the following command.

AT+LGETDATA	+LGETDATA:1234,-64,27,1

In this case the data sent by the server was 1234.

5. UART INTERFACE CONTROL PROTOCOL (UICP)

5.1. General Protocol Description

Telit UART Interface Control Protocol (UICP) defines a protocol to control the logical state of an UART based interface, thereby peers to switch off local UART devices for power saving (or other) reasons.

The UICP+ is a bi-directional, symmetrical protocol that allows to negotiate UART interface states with a communication partner connected via UART by using of standard UART signal lines.

The UICP+ mechanisms defined here enable the involved peers to negotiate UART interface states by signaling the remote peer it is allowed to enter or exit an UART interface up state.

The UICP+ does not enforce any power saving support of the involved peers but implements mechanisms to allow the save usage of MCU power saving features like UART peripheral switched off.

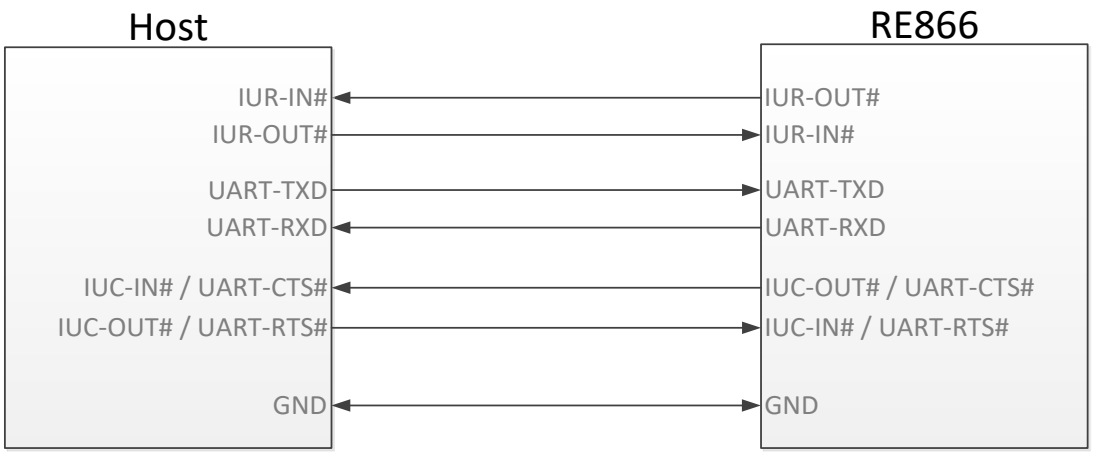
5.2. Requirements of Using UICP on RE866

To make use of UICP, the lines UART-TXD, UART-RXD, UART-RTS# (IUC-IN#), UART-CTS# (IUC-OUT#), IUR-OUT# and IUR-IN# should be connected between RE866 and the host and additionally the UICP protocol should be implemented on host site.

A detailed description of implementing UICP is described in the document *UICP+ UART Interface Control Protocol [4]*.

To activate UICP on the RE866 the configuration parameter AT+UICP=1 needs to be set (followed by AT&W and AT+RESET).

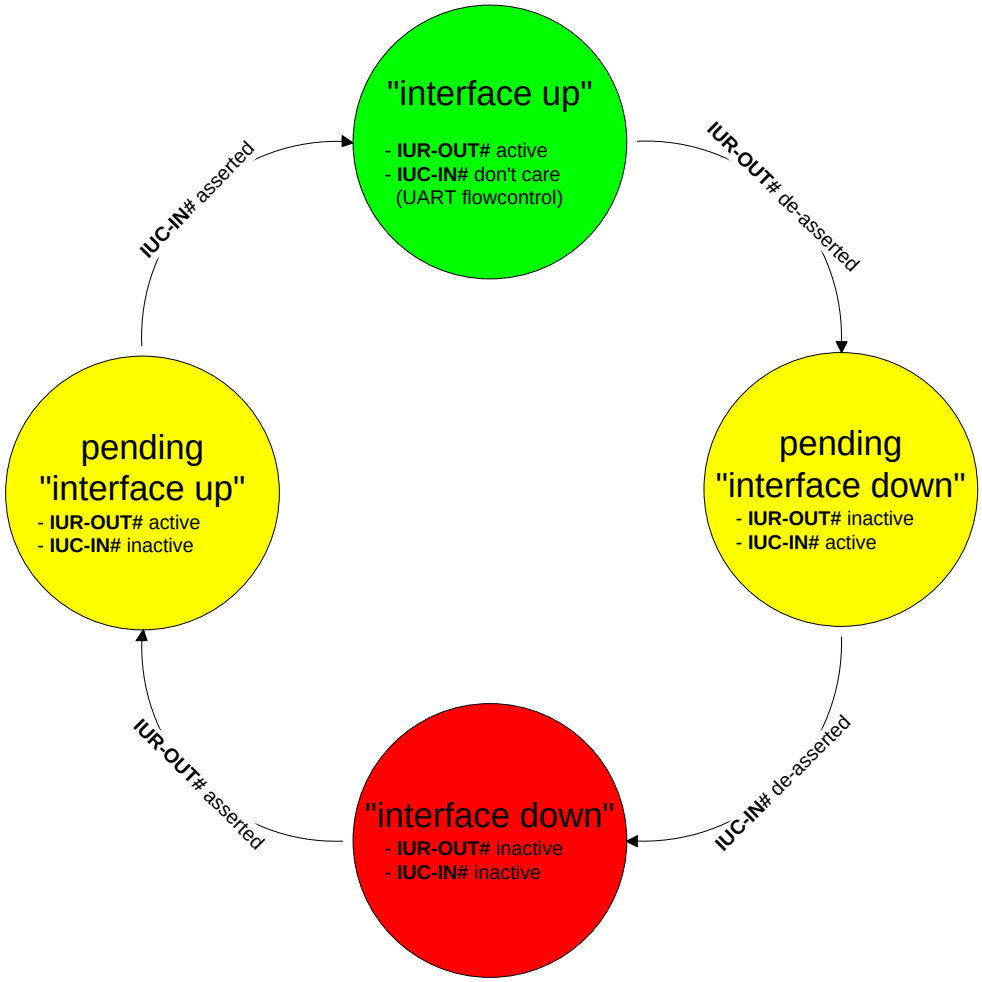
5.3. Connection Example between RE866 and Host Controller



Further information about the RE866 UART interface is described in the document *RE866 Hardware User Guide [1]*.

5.4. UICP Protocol States

The UICP protocol defines four states:



- **interface up**
  normal operation, RTS/CTS hardware flow control is active
- **pending interface down**
  IUR-OUT# is requested to go to “interface down” state
  IUC-IN# is not confirmed
- **interface down**
  IUR-OUT# and IUC-IN# are de-asserted in “interface down” state and can enable MCU power saving
- **pending interface up**
  IUR-OUT# is requested to go to “interface up” state,
  IUC-IN# is not confirmed

All data received before the interface up state has been achieved shall be seen as invalid data and shall be discarded.

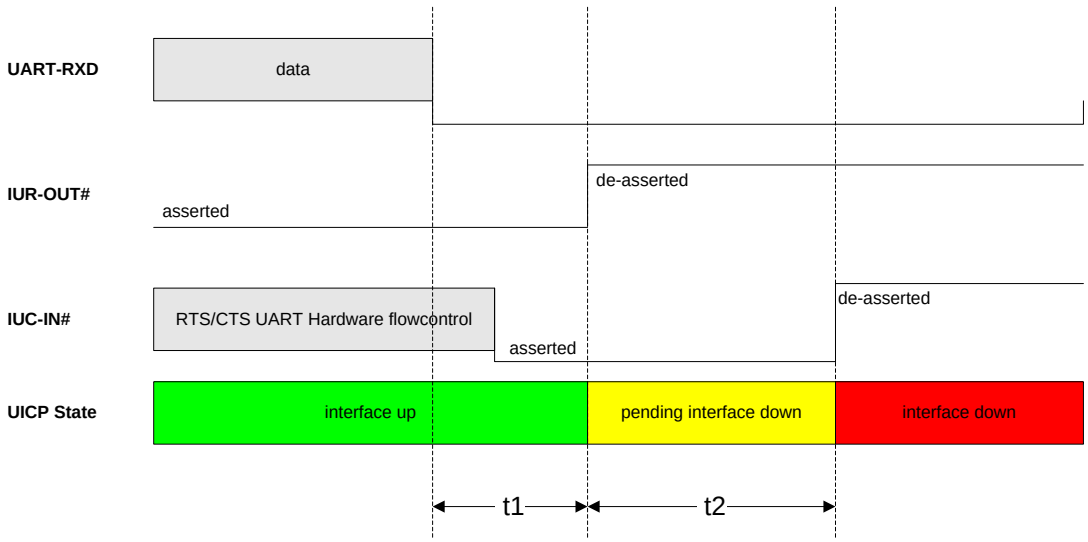
After reset in activated UICP configuration the initial state is “interface down”, in case of non connected host RE866 remain in “interface down”.

5.4.1. Drive from “interface up” to “interface down” State

Once a de-asserted IUR-OUT# signal of the initiator is detected by the acceptor, the acceptor shall confirm that signal by de-asserting its IUC-OUT# signal which is connected to the IUC-IN# signal of the initiator.

After the initiator detects a de-asserted IUC-IN# signal both devices go into “interface down” state and can enable MCU power saving mechanisms.

During MCU power saving, the MCU can switch off the UART but shall be able to detect an IUR# assert.



t1 >= 100 ms (see this chapter)

t2 < 1 s

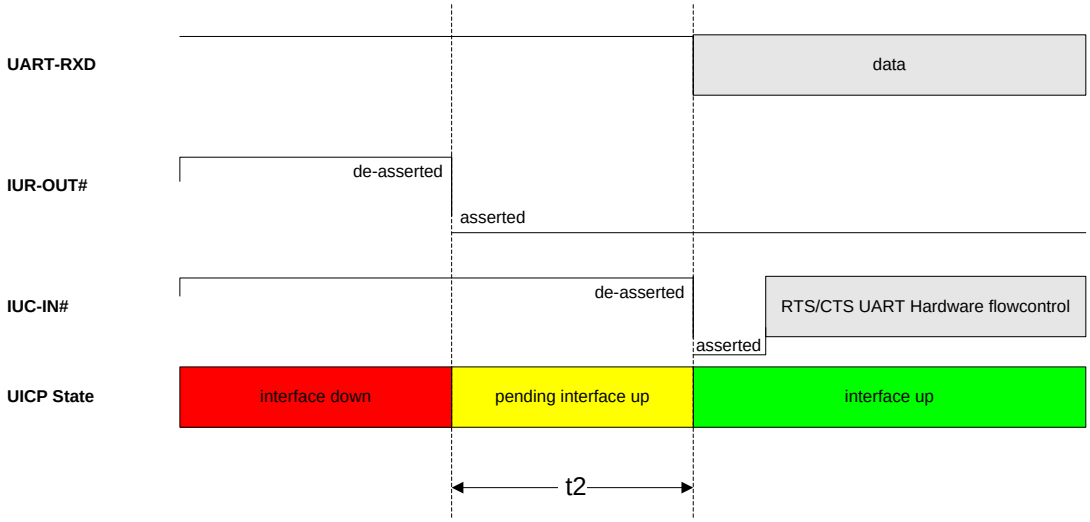
5.4.2. Drive from “interface down” to “interface up” State

To initiate the state change from “interface down” state to “interface up” state the initiator shall assert the IUR-OUT# signal.

The acceptor confirms the IUR-IN# signal with asserting its IUC-OUT# signal which is connected to the IUC-IN# signal of the initiator.

Once the acceptor detects the assert of the IUR-OUT# signal from the initiator, it can disable MCU power saving mechanisms but shall ensure the UART is ready to receive data before it confirms asserting its IUC-OUT# signal which is connected to the IUC-IN# signal of the initiator.

Once the initiator detects the assert of the IUC-IN# signal of the acceptor, the in initiator can send data to the acceptor.



5.5. Example of UICP Usage

The following examples shows the state change between the RE866 and the host.

The scenario here might be that both devices use the “interface down” state to drive the MCU into some kind of power saving mode that allows to “wake up” the MCU with external GPIO signals.

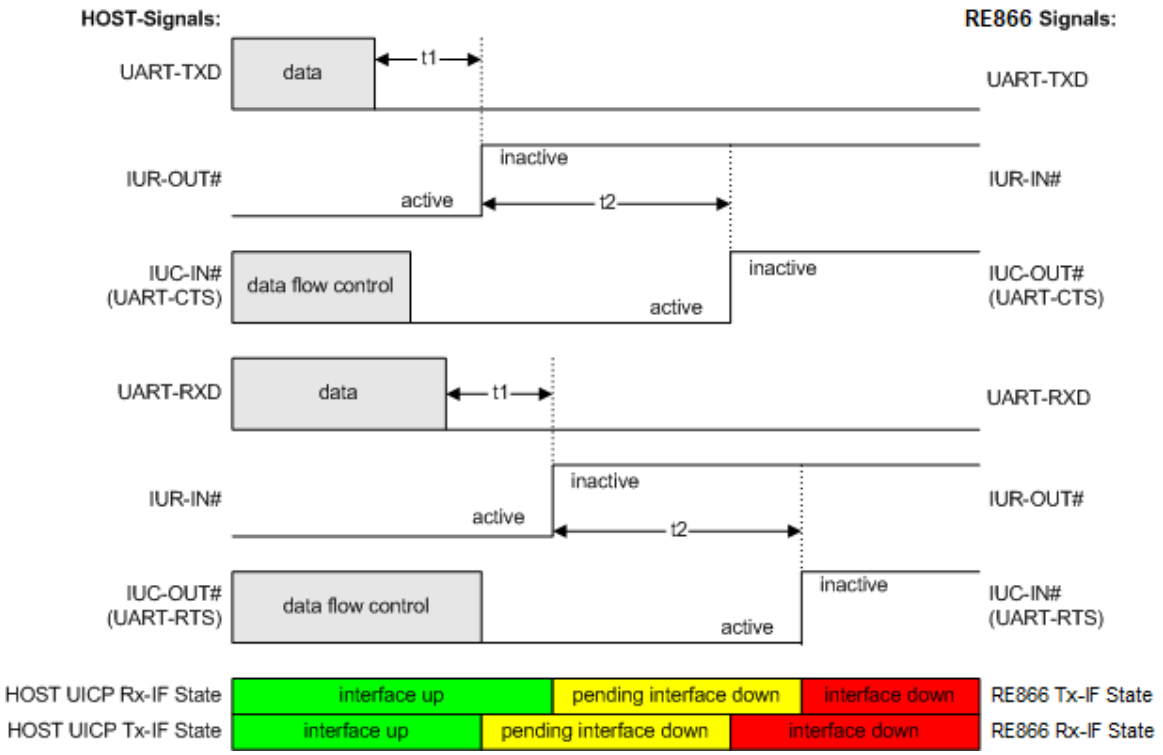
5.5.1. State Change from “interface up” to “interface down”

Host and RE866 are in the state “interface up” and exchange bidirectional data. After the host has send all data and is idle for **t1** in its Tx direction it signals the RE866 it is allowed to go to “interface down” state by de-asserting IUR-OUT# signal.

Parallel to that UICP signaling from host to RE866 the RE866 has send all data as well and is idle for **t1** in its Tx direction, so it signals the host it is allowed to go to “interface down” state by de-asserting IUR-OUT# signal.

The host and the RE866 each wait for a maximum time **t2** to detect the de-asserted IUC-IN# signal. After receiving this input change via the IUC-IN# signal both devices may change from state “pending interface down” to state “interface down”.

Both UICP signaling sequences proceed in parallel until host and RE866 interfaces are in “interface down” state.



5.5.2. State Change from “interface down” to “interface up”

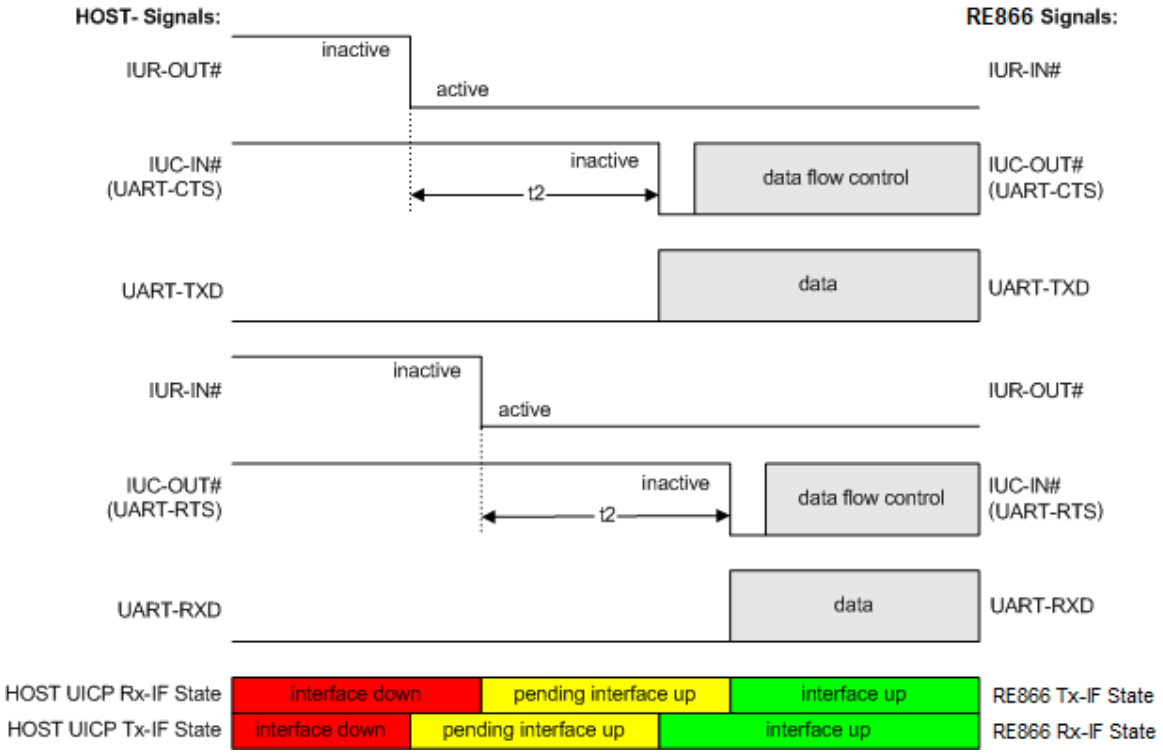
Host and RE866 are in the state “Interface down” and may have the MCU into some kind of power saving states.

The host wants to send data to the RE866 and asserts its IUR-OUT# signal.

Parallel to that UICP signaling from host to RE866 the RE866 wants to send data to the host and asserts its IUR-OUT# signal as well.

The host and the RE866 each wait for a maximum time **t2** to detect the assertion via the IUC-IN# signal. After receiving this input change of IUC-IN# both devices may assume that the interface of the remote device changed from state “pending interface up” to state “interface up”.

Both UICP signaling sequences proceed in parallel until host and RE866 interfaces are in “interface up” state and data can be exchanged bidirectional.



6. SYSTEM OFF MODE

The RE866 supports the possibility to set the module into low power mode during the time the module is not used with the AT+SYSTEMOFF command.

Syntax: AT+SYSTEMOFF=<value>

Value	Description
1	Wake up by GPIO (UART-RTS#) or RESET signal
2	Wake up by RESET signal only

Depending on the value the RE866 will restart either on activity at the GPIO input line UART-RTS# and/or after RESET signal.

It is possible to monitor the UART flow control line UART-CTS# to detect a “module ready” state.

6.1. Using System OFF Mode for Terminal I/O

The following example will list the communication between the host controller and the RE866 using the integrated Terminal I/O profile.

To set the RE866 into the low power mode the host controller needs to send the AT+SYSTEMOFF command. The following examples based on AT+SYSTEMOFF=1.

The RE866 will respond “OK” before changing into low power mode.

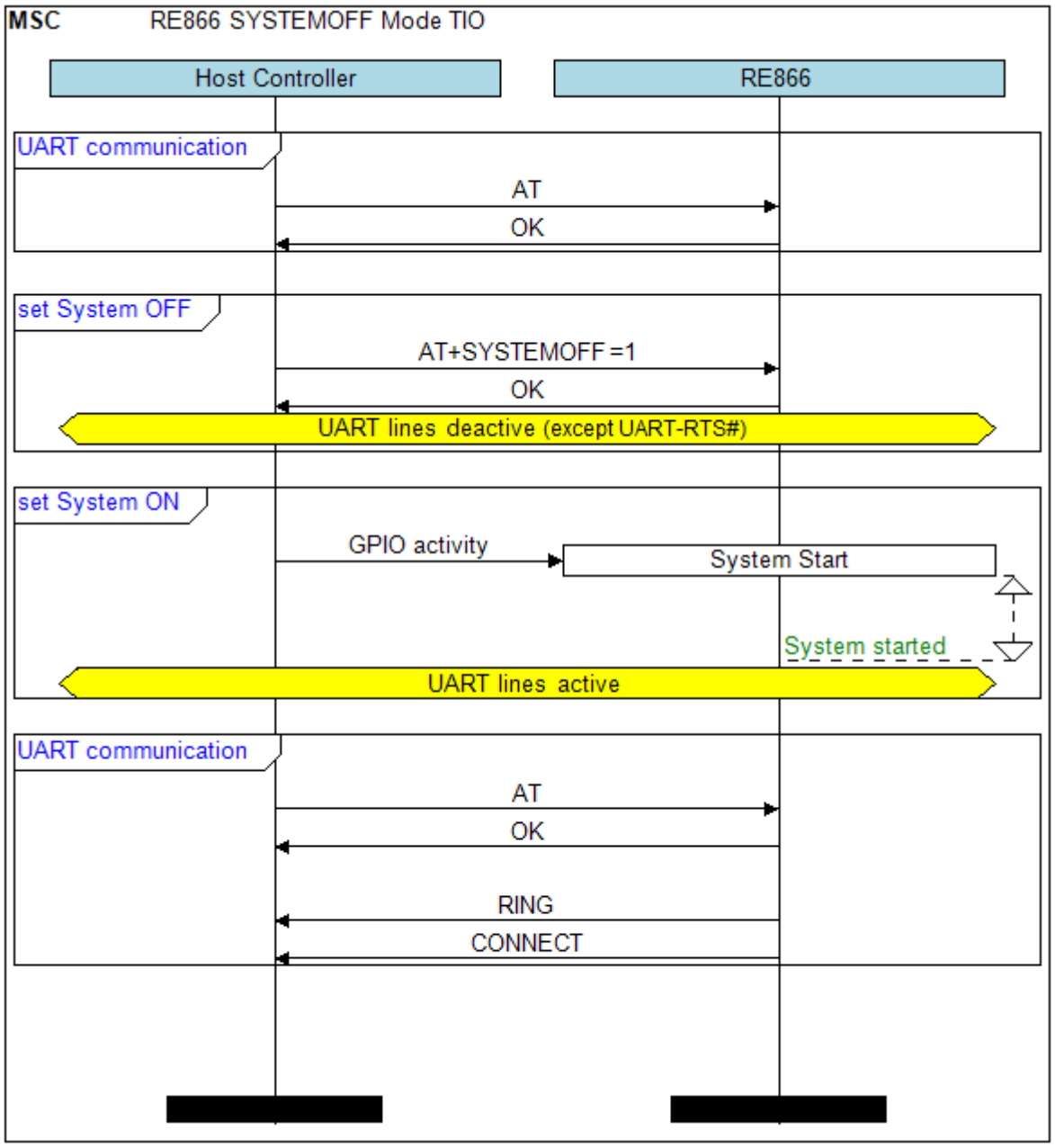
To activate the RE866 from low power mode the host controller needs to activate one of the following GPIO lines:

- UART-RTS# (pull RTS to high level to wake up from SYSTEMOFF)
- RESET signal (pull RESET to low level to wake up from SYSTEMOFF)

The module detects the GPIO change and starts the firmware.

After the firmware is started (see also “Startup Timing” in chapter 3.3) the host can continue the UART communication.

An incoming call is reported with RING and CONNECT.


MSC
RE866 SYSTEMOFF Mode TIO
Host Controller
RE866
UART communication
AT
OK
set System OFF
AT+SYSTEMOFF =1
OK
UART lines deactive (except UART-RTS#)
set System ON
GPIO activity
System Start
System started
UART lines active
UART communication
AT
OK
RING
CONNECT

7. FIRMWARE UPDATE

The firmware update of the RE866 can be done locally by either

- A Telit provided firmware update tool. This is a Windows™ program that contains the firmware and uses a PC with a serial port for the update
  Implementing the firmware update protocol on the host system
  or over the air via Bluetooth LE.

7.1. Serial Firmware Update

7.1.1. Prerequisites for Serial Firmware Update

You need to have access to the UART interface of the RE866.

Serial firmware update requires at least the serial lines UART-RXD, UART-TXD, UART-CTS#, UART-RTS# and GND.

Serial firmware update requires a UART speed of 38400 bps.

Pin BOOT0 (E-1) shall be pulled high to access the bootloader at start-up.

7.1.2. Telit IoT Updater

The firmware update will be done by a Telit provided firmware update tool. This is a Windows™ program that contains the firmware and uses a PC with a serial port for the update.

For example, a firmware version V1.1 will result in the executable file “RE866A1-EU_BT_V1_1_xxxx_FWupdate.exe”.

The software used for the upgrade is able to run on the following Win32/Win64 platforms:

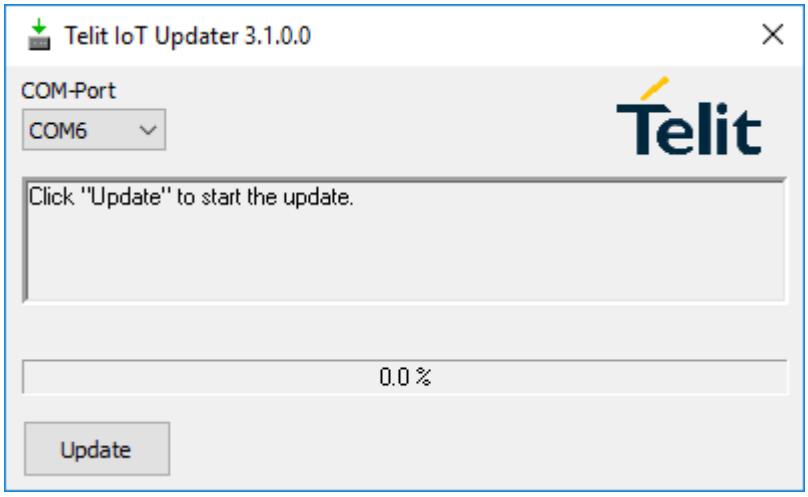
- Windows 7
- Windows 8
- Windows 10

Testing was carried out on Windows 10 Pro, Windows 8 Pro and Windows 7 Ultimate 64-bit platforms; however experience suggests that the described software runs on all Windows 10 / 8 / 7 32 and 64-bit platforms.

The program requires a PC with at least one free COM port.

The upload is processed via the serial port the device is attached to.

Before starting the update by pressing the “Update” button the device shall be reset.



- COM-Port
  The COM port the device is attached to
- Update
  Starts the update procedure

After the successful update close the software, remove the high level on pin BOOT0 and reset the RE866.

Do not disconnect the device while the update is in progress, otherwise the update will fail and has to be repeated. In case it is not possible to update the RE866 please contact the Telit support (mailto:ts-srd@telit.com).

7.2. Firmware Update Over the Air (OTA)

The RE866 supports firmware over the air update. The firmware update over the air can be performed by using the Nordic nRF ToolBox app available for iOS and Android or by using the Nordic Master Control Panel and the corresponding Nordic Bluetooth hardware.

The firmware over the air update in the RE866 will be enabled with the commands below:

- AT+DFUMODE=2
- AT+DFUSTART

After sending the AT+DFUSTART command the RE866 is visible in the air as “RE866DFU” (name configured with command AT+DFUNAME) for a time period of 2 minutes. If no firmware update is performed during this time the RE866 will continue with normal operation.

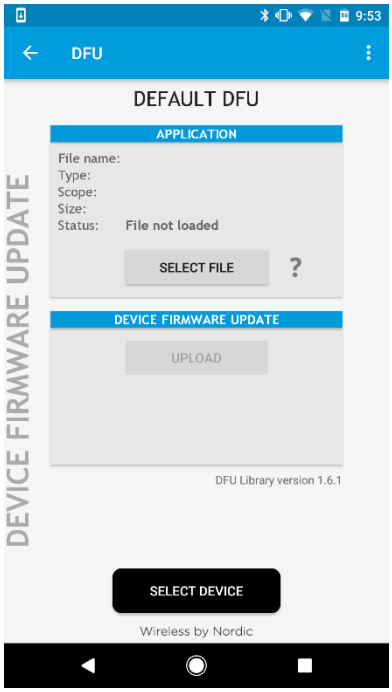
The following chapter describes the firmware over the air update by using the Nordic nRF Toolbox app on Android

7.2.1. OTA FW Update using Nordic nRF Toolbox on Android

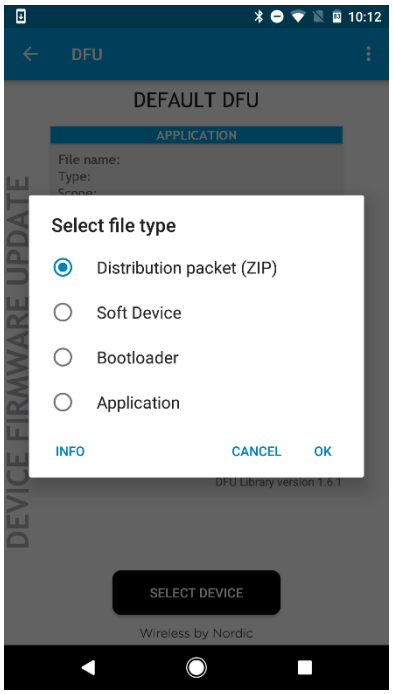
Make sure the RE866 has already activated the firmware over the air update.

Open the nRF ToolBox app on the smartphone and choose “DFU“.

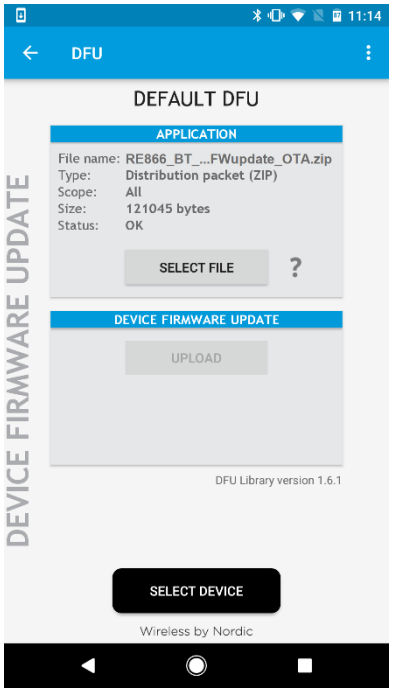
Press the button “SELECT FILE”.



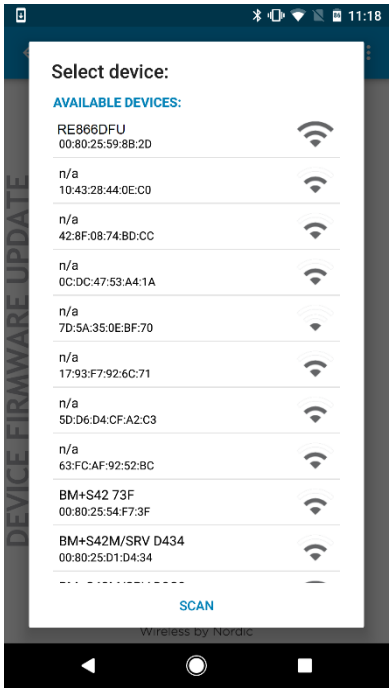
Select file type “Distribution packet (ZIP)”.



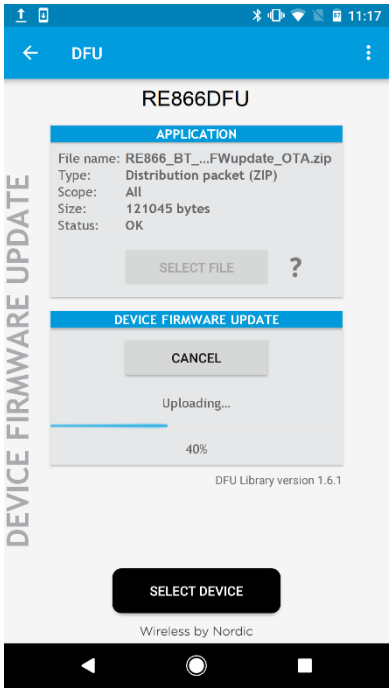
Search via file manager for the firmware package which was previously copied to the smartphone (e.g. RE866A1-EU_BT_V1_1_xxxx_FWupdate_OTA.zip in the example below).



Press the button “SELECT DEVICE” and select the “RE866DFU” from the list of available devices.



Press the “UPLOAD” button to upload the firmware package over the air to the RE866.



After the file was uploaded successfully the RE866 will start with the new firmware.

8. GLOSSARY AND ACRONYMS

AT	Attention Command
GAP	Generic Access Profile
GATT	Generic Attribute Profile
SSP	Secure Simple Pairing
UART	Universal Asynchronous Receiver/Transmitter
UICP	UART Interface Control Protocol
UUID	Universal Unique Identifier

9. DOCUMENT HISTORY

Revision	Date	Changes
0	2018-05-03	First issue

SUPPORT INQUIRIES

Link to **www.telit.com** and contact our technical support team for any questions related to technical issues.

www.telit.com

Telit Communications S.p.A.
Via Stazione di Prosecco, 5/B
I-34010 Sgonico (Trieste), Italy

Telit IoT Platforms LLC
5300 Broken Sound Blvd, Suite 150
Boca Raton, FL 33487, USA

Telit Wireless Solutions Inc.
3131 RDU Center Drive, Suite 135
Morrisville, NC 27560, USA

Telit Wireless Solutions Co., Ltd.
8th Fl., Shinyoung Securities Bld.
6, Gukjegeumyung-ro8-gil, Yeongdeungpo-gu
Seoul, 150-884, Korea

Telit Wireless Solutions Ltd.
10 Habarzel St.
Tel Aviv 69710, Israel

Telit Wireless Solutions
Technologia e Servicos Ltda
Avenida Paulista, 1776, Room 10.C
01310-921 São Paulo, Brazil