DOCUMENTATION

LST LoRa Setup Tool

INNOTAS ELEKTRONIK GMBH

11 Dezember 2019

Written by: Dipl.Ing.S.Sieber

1 Table of Contents

2 Revision directory

REVISION	DATE	MODIFICATION
1.0	Dezember 2019 11	First edition
1.1	01/23/2020	Revision Töpfer

3 Usage

The LoRa setup tool from Innotas Elektronik is a Windows® program for reading out and parameterizing LoRa devices from Innotas. As of December 2019, this includes the devices LoRa water meter, LoRa EHCA and LoRa pulse module.

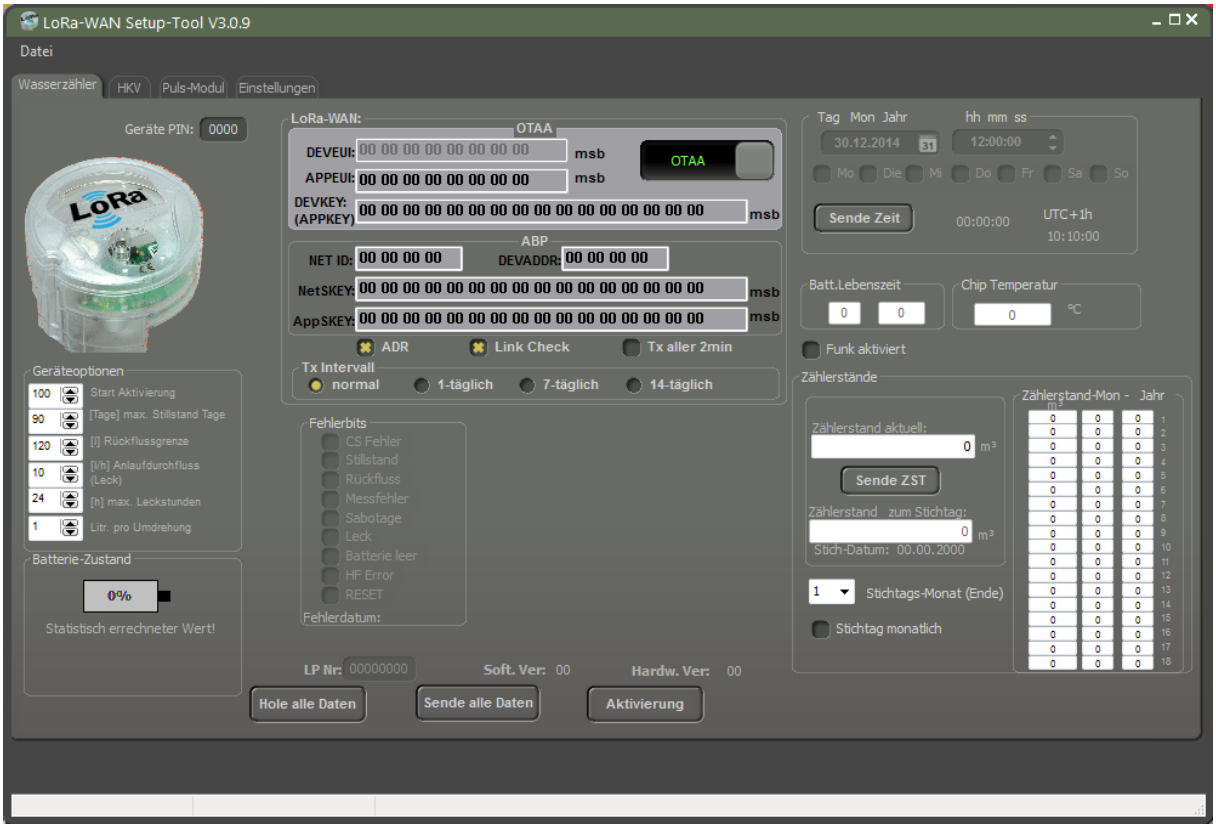
4 Safety instructions

The use of the LST is only recommended for qualified personnel who are familiar with the exact function of the devices and who recognize and anticipate the consequences of a new parameterization. After re-parameterizing devices, we strongly recommend that you test for proper function. Furthermore, possible consequences of changing meter readings or cut-off times must be observed. Incorrect configuration can shorten the battery life or impair the accessibility via the gateway. Innotas assumes no guarantee in the event of improper interventions.

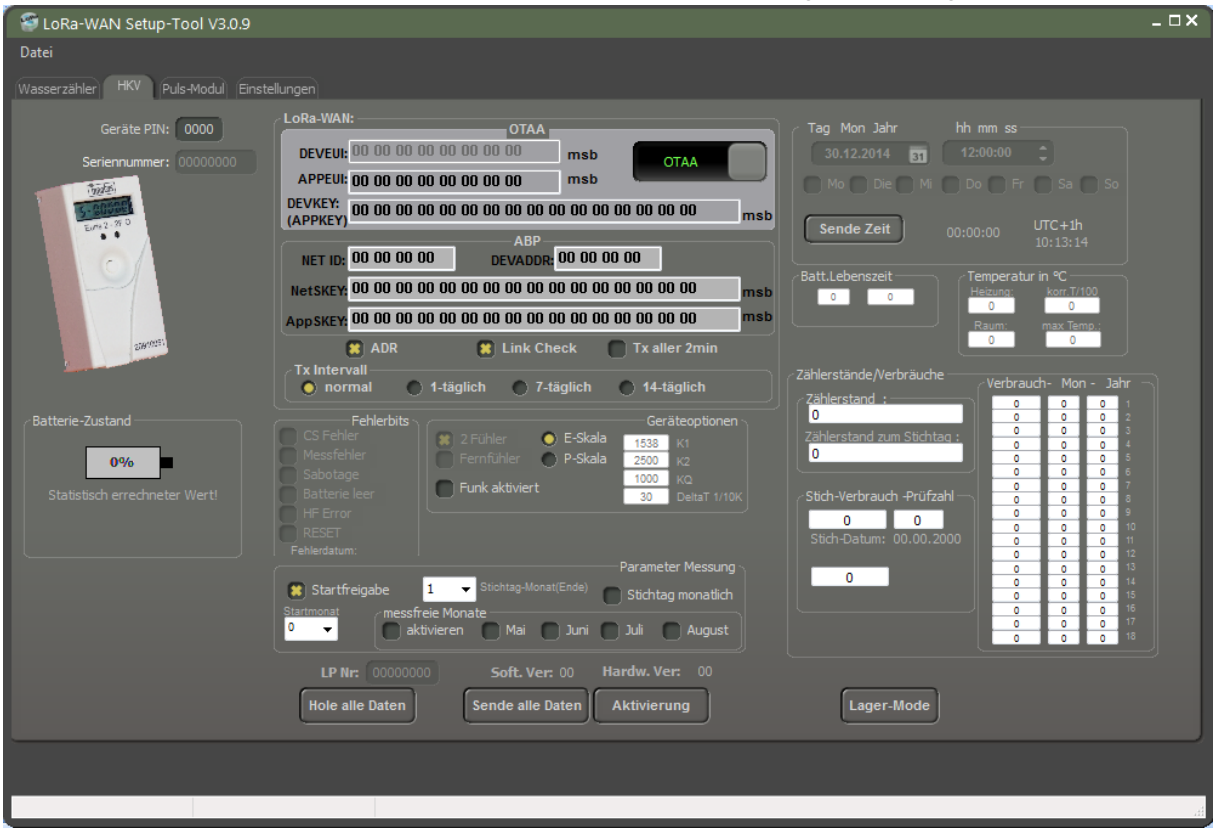
5 General information on communication with the LoRa device from Innotas

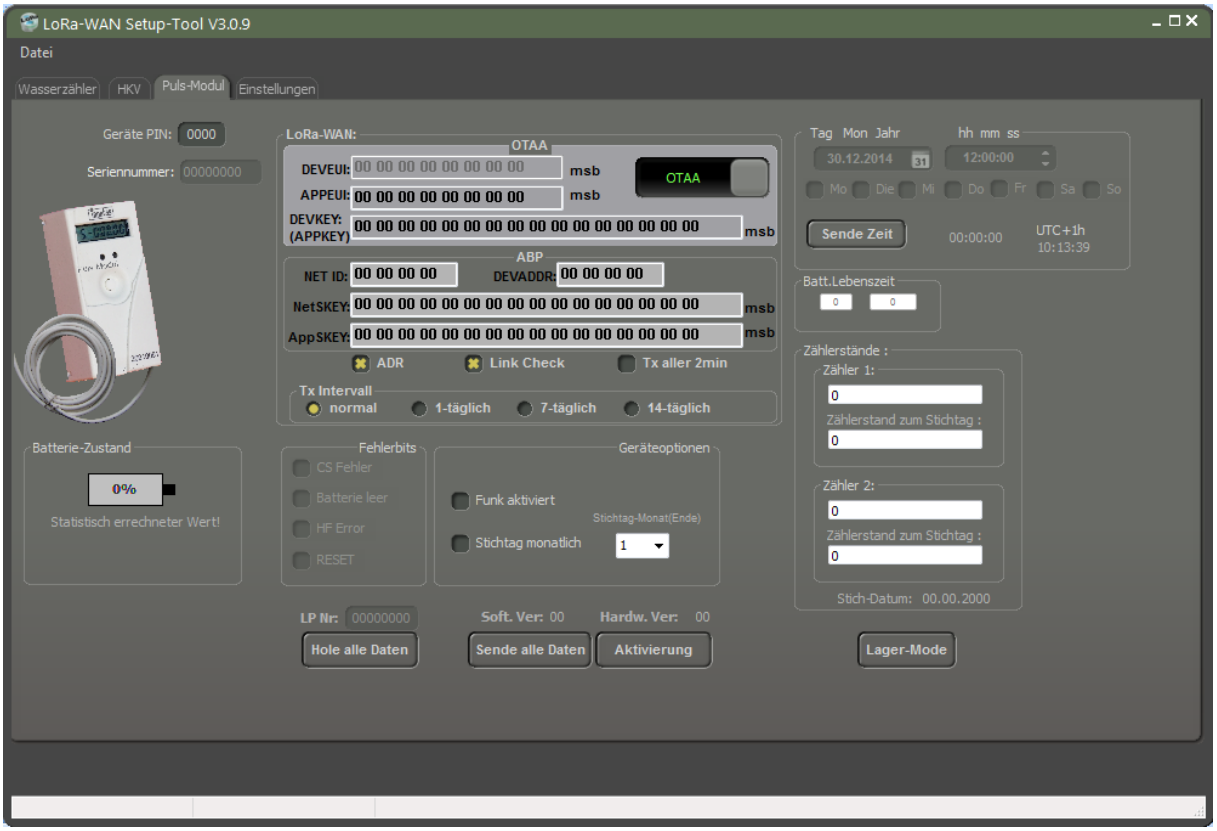
The LoRa devices have an IrDa interface with which communication for reading out and parameterizing is possible. The physical interface parameters are RS232 8, n, 1 with 2400 baud.
A commercially available optical head with a USB interface is recommended as an adapter. This can be ordered via Innotas Elektronik GmbH. All devices use the same communication frame, just with different commands. The hardware version and the respective software version are also transferred. A device PIN can be used to protect against access by unauthorized persons.
The device PIN has 4 digits and is deactivated at the factory using the number sequence “0000”. The PIN can be changed by the user via the opto head or via the LoRa return channel.

6 Start LoRa Setup Tool



The LoRa setup tool has 4 tabs. One tab for each type of device and one for general settings.





6.1 Settings in the LST

The following settings can be made:

- The COM interface of the opto head

- the wake-up preamble for all devices except the compact EHCA

- the device PIN to be used

- the offset to be used for the PC time that is to be used for programming the device time

The settings used are saved when the program is closed and used again the next time it is started.

6.1.1 COM interface

All UART interfaces listed in the system are displayed in the folding box. Not all interfaces shown are also physically and operational at the moment. They are partly virtual UARTS from other utilities. To determine the COM of your opto head, plug in the opto head and press the refresh button with the "R". All available UARTS are then read in again. You should now also see the COM of your attached opto head. Then select it from the list. If necessary, you can also determine the interface via the Windows device manager.

6.1.2 Wake up preamble

The interfaces of the water meter and the EHCA in the long version (the model without a button) must be "woken up" for communication. This is done by a special wake-up sequence before communication. Since the EHCA with key is woken up by pressing a key, the preamble is not necessary there, but not incorrect. Communication takes about 2 seconds longer.

6.1.3 Device PIN

The activated device PIN prevents the use of the optical interface by unauthorized persons. The PIN is deactivated at the factory with "0000", so it is not requested by the device. The device PIN set here is used for every further communication request. It is therefore recommended to save them securely or to use the same PIN for several devices.

Note: The PIN of each device can also be changed via LoRa, i.e. set or deactivated by writing "0000". Please note: If a PIN> "0000" is set in the device, the pin is active. Then the set PIN must be entered in the **Settings tabs** for further communication with the device!

6.1.4 Temporal offset

The time offset relates to the set PC time.

If, for example, "-1" is selected, the clock is set one hour earlier, i.e. to 7:00 am if the PC time is 8:00 am. Different time zones and summer / winter time can be taken into account.

7 Settings for the LoRa radio communication

7.1 General explanations

LoRa communication is protected with 2 AES keys. First, the user data (meter readings, etc.) are encrypted with an AppSKey. This data is supplemented by the communication layer of the LoRa-WAN and then all encrypted together with the NetSKey. This enables a separation between communication in the network and processing of the user data. For this purpose, the LoRa server forwards the encrypted user data to the application server, which in turn is able to decrypt and process this data.

7.1.1 Terms

DEVEUI	Unambigous unique ID of the device according to the IEEE standard
APPEUI	Unambigous unique ID of the device type on the server
DEVKEY	Public key for use when JOIN via OTAA
NetSKEY	Private key to encrypt all data before communication
AppSKEY	Private key to encrypt all user data before it is integrated into the communication protocol
NET ID	Number of the network to which the device is connected
DEVADDR	Short numbering / labeling within the connected network
ADR	Automatic data rate setting, the spreading factor is changed by the device itself
Link check	Control of the existence of a connection

7.1.2 Establishing a connection with the LoRa network

There are two ways to connect to the LoRa network, OTAA or ABP. The route preset in the end devices at the factory is **OTAA**. The device is preset with DEVEUI, APPEUI and DEVKEY at the factory. This data is transmitted to the customer electronically. He makes this known to the network server himself or through a service provider.
The measuring device is attached and put into operation (activated). The meter begins with a JOIN sequence. The data is encrypted with the public key. A server that receives this data checks whether it can decrypt it and whether this device is listed with it. If so, he negotiates new private keys with the device and receives the DEVADDR and Net ID from the measuring device. From this point on, the device uses the private keys for communication, NetSKEY and AppSKEY, which were transmitted by the server.

When establishing a connection with **ABP**, the negotiation of the private keys is skipped and these must have been programmed into the system (server) before commissioning. This method offers little flexibility when integrating into a network.

7.1.3 ADR (automatic data rating)

The measuring device changes its data rate via ADR depending on the reception quality. It receives the reception quality from the server via the acknowledgment protocol. A slower connection (large spreading factor) has a greater range, but a higher network and battery load. If the reception quality is poor, the device automatically changes the spreading factor step by step from SF7 to SF12. If the device is repeatedly received very well, the server, with the appropriate setting, sends the device a command to lower the spreading factor again.

7.2 Measurement data transmission

The transmission interval of the devices is 2-4 hours in the "normal" case. Depending on the device and the spreading factor, the devices transmit at intervals of 2-4 hours. With spreading factors of SF11 or SF12, the transmission intervals are extended.
Since the devices are operated in stationary operation, intervals> = 1 day are usually sufficient. Therefore, the

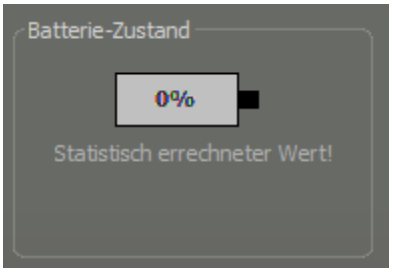
transmission frequency can be limited to one telegram per day. If even less measurement data is required for data protection reasons, the transmission of measurement data can be limited to once a week or once every 2 weeks. In this case, an empty telegram is sent during the intervening days, which only contains the device status. This maintains the network's ability to react. Immediately after activating the radio and successfully establishing a connection via JOIN, the devices send a telegram every 2 minutes for a few hours. This mechanism is used to get quick feedback from the LoRa server on site after the device has been installed as to whether the commissioning was successful.

7.3 Activation

The devices are usually activated by an activation sequence via the Irda optical head activated. Some devices also have a self-activation. After activation, the radio is activated in the device. However, this does not yet indicate whether the device is also connected to a server. The activation can be repeated as often as required. Please note, however, that repeated sending of the telegrams every 2 minutes has a negative impact on the battery budget and at the expense of the forecast service life.

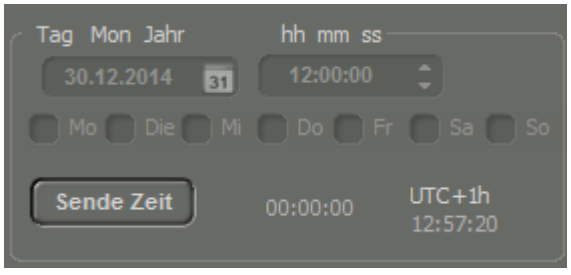
8 Energy display

The battery life of the devices is designed for a certain time under assumed conditions. The frequency of transmission and the spreading factors used represent the largest variables. Further uncertainties are connection interruptions, radio interference, server failure, etc. The network server requires a battery status from the device at a certain time interval. To determine battery health, statistical values in the device are used, among other things.



9 Date / time

The time of the devices can be changed using a separate button. Only the new time is sent to the device. The time to be sent is calculated as an offset from the current PC time and the number of hours entered under Settings. With this you can, for example, program the devices for winter time without changing the PC time. If the device is read out using the "Get data" button, the current time in the device is displayed here.



10 Read out device

With the button „get all data“ all data are read out from the device. Note: This should be done each time before changing individual device settings to prevent settings that should not be changed from being overwritten.

11 Change and write data

Before changing individual data in the device, the device must be read out completely in order to make individual changes based on these settings. With the button 

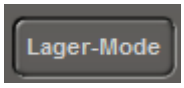
all data is written to the device. In the event of changes to meter readings and due date times, the plausibility of the following value acquisition must be checked.

12 Changing the counter reading of water meter attachments

The LoRa water meter attachments can be delivered as a unit with a water meter on request. The mechanical meter readings are compared with the electronic meter reading ex works. If the water meter attachments are first connected to water meters on site, a comparison of the meter reading may be desirable. The water meter window has an extra button to speed up the process. 

A meter reading can be entered here directly. Other settings are not changed. It is therefore not absolutely necessary to read out all device data beforehand.

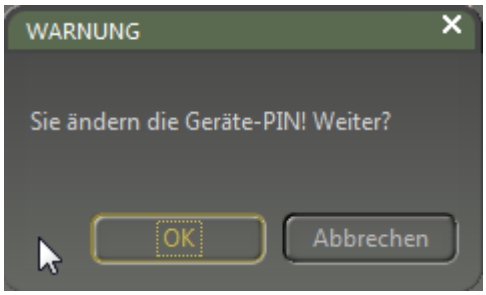
13 The storage mode

The devices are delivered without activated radio. The EHKVs and pulse modules are even in a "storage mode". Neither the radio nor the measurement is activated. These devices can be switched to this inactive storage mode again after activation using the "Storage mode" button. 

14 Change the device PIN

After reading out a device, the read out PIN is displayed in the top left of the window. 

. To change the device PIN, enter the required new PIN here and send all data to the device. A safety notice is given.



A device can only be read out if the PIN in the device is deactivated by PIN "0000" or if the active PIN is entered in the "Settings" tab.

14.1 Water meter with high power

The "normal" LoRa modules support a transmission power of approx. 14 dBm from the HF chip. A significantly lower transmission power is emitted with the small antenna due to the installation space. We also offer the water meter attachments as a high-power version. This means a transmission power increased by approx. 6 dBm, which is achieved by feeding more transmission power into the antenna. However, this reduces the number of possible send telegrams to a maximum of one telegram per day. When reading out the water meter, the image of the water meter attachment shows that it is a high-power module.