# *iNode LoRa*

# *GSM MQTT*

***LORA – GSM gateway***

***user manual***

*© 2018-2020 ELSAT ®*

# 1. INTRODUCTION

We would like to introduce you to the family of iNode devices operating in LoRa® technology and with the **LoRaWAN** protocol.

**iNode LoRa GSM MQTT** allows the existence of devices working in LoRa® technology in networks with the IP protocol: GPRS, MQTT and the Internet.

*Based on Wikipedia about LoRa® :*

*LoRa® (Long Range) uses license-free sub-gigigahertz radio frequency bands (so-called ISM band), such as 169 MHz, 433 MHz, 868 MHz (Europe) and 915 MHz (North America). The data transmission rate in the LoRa® system is between 0.3 kb / s and 37.5 kb / s. Because of the techniques used to minimize the use of energy, LoRa® is not suitable for real-time services, but only for applications in which delays can be tolerated.*

*The adopted network topology is the so-called star-of-stars - the central element is surrounded by intermediate elements - so-called gateways, which communicate with end devices. The higher the number of end devices in a cell, the lower the network throughput.*

*In the radio layer, LoRa® uses the CSS (chirp spread spectrum) modulation technique developed by Semtech , which has the ability to receive a signal below the noise level.*

*Pros and cons*

*LoRa® modulation is characterized by low energy demand of the device used for communication. This protocol adapts the transmitter power and transmission speed to the current propagation conditions (wave propagation). In practice, this means a long working time of the sensor on one battery.*

*LoRa® modulation has a range of up to several kilometers. In this respect, it prevails over solutions such as Bluetooth and WiFi.*

*The use of LoRa® technology does not involve license fees for frequencies. The technology LoRa® used unlicensed frequency band (433 MHz, 868 MHz and 915 MHz). The technology LoRa® can connect multiple devices, making this protocol suited for use as a communication solution for cities.*

*The downside of LoRa® modulation is the speed of data transmission. It is in the range of 0.3-37,5 kbps. It prevents devices from sending large data, but allows the sensor network to work.*

*Another limitation of the LoRa network is the high price of communication modules.*

Trademarks or registered trademarks:

*Lora®, LoraWAN®, Bluetooth ®, Windows, Android, Google, Microsoft, Chrome, Linux, Murata, Semtech, ST are used in this brochure for informational purposes only and belong to their respective owners.*

**Please read this manual carefully before starting the installation! We cannot take responsibility for damages resulting from improper use of the device.**

**Warning**

**This device is a class A device. In a residential environment it may cause radio interference. In such cases, the user may be required to take appropriate countermeasures.**

# 2. SAFETY INFORMATION

**Please read the safety information before switching on the device.**

## 2.1 Power source

The device can be connected to the AC 230V 50Hz AC power network only with 230V AC / 5V DC stabilized power supply with double or reinforced insulation and output over-current protection. The nominal value of this current can not be greater than 2.1 A.

## 2.2 General conditions for safe use

- The device should be located in a safe and stable place.
- The external power supply should be placed in an easily accessible wall socket (e.g. not hidden behind furniture). Some power supplies of this type do not have their own power switch, so disconnecting them is only possible by removing them from the wall socket completely.
- Do not use external power supplies outside the building or in places with high humidity.
- When using a device with an external power supply, make sure that the cable is positioned so that it is not exposed to being trampled on, hooked or pulled out of the power supply by persons or animals moving around the room.
- Do not place the device or the adapter on a wet surface. Do not use in a humid environment. Do not allow wetting: e.g. rain through an open window. Never place containers with liquids on the device or power supply: vases, glasses, cans, glasses etc.
- Never place an open flame on the device or power supply: candles, oil lamps, etc.
- If you notice any damage to the power cord or plug, please contact a service center immediately to resolve the problem.

## 2.3 Cleaning

- Before cleaning, always unplug the machine by unplugging the power cord or adapter from the power outlet.
- Do not use liquid cleaners or aerosol cleaners.
- For cleaning only use a dry, soft, lint-free cloth.

## 2.4 Ventilation

- All openings and slots in the housing of the device or power supply are for ventilation. They must not be covered or covered, as it may overheat the internal components.
- Protect the device and power supply against access of small children able to throw small things into the ventilation holes

## 2.5 Service

- If necessary, take the device to a specialized service center. There are no user serviceable controls or useful components inside.

## 2.6 Before commissioning

- Before starting the installation, check the compliance of your mains voltage with the information on the device or power supply.
- Switching the power on and off from the power socket is always carried out by holding the plug or the power supply housing, not the power cord.
- If only the power cord plug or adapter is in the wall socket, the device is still powered. The DC power plug is the only element that disconnects power from the device.
- If anything falls or falls inside the machine or the power supply, immediately remove the plug from the wall socket. The device or power supply unit may not be used until an expert inspection has been performed.
- Do not disassemble the device or power supply. There may be dangerous voltage inside, threatening health and even life. Any repairs and adjustments inside should only be performed by qualified service personnel.

## 2.7 Location

- Place the device and power supply in a place with good ventilation - free air flow. This will prevent internal components from overheating.
- Never place the device or the power supply near heating devices or in sunny places.
- Never place heavy objects on it.

## 2.8 Steam condensation

Under certain circumstances (e.g. sudden change of location from a cold to a warm room) the device and / or the power supply may become covered with steam, preventing the device from being used temporarily. In this case, wait about 1 hour for the temperature of the device to stabilize and the moisture to evaporate.

## 2.9 Connecting iNode LoRa GSM MQTT

To launch **iNode LoRa GSM MQTT** in a GPRS/GSM network, follow these steps:

- Connect the GSM antenna to the device (Fig. 1). If it has a radiator, it should be placed vertically.
- Install the **iNode LoRa Monitor** application to configure sensors from the **iNode LoRa** family: **iNode LoRa EM**, **iNode LoRa T**, **iNode LoRa HT**. Thanks to the WebUSB functionality, it works in Chrome or Chromium browsers on various operating systems, such as Android OS, Linux or Windows 10, and works directly with USB adapters: **iNode LoRa USB** or **iNode LoRa GSM MQTT** . In other browsers, e.g. FireFox, it is necessary to use the **iNode Hub Serve**r application for Windows 10. **iNode Hub Server** is also necessary for **iNode LoRa GSM** with mini USB connector with FTDI chip.

**ATTENTION !!! Do not tilt the antenna radiator if it is tightened to the device, otherwise it may be damaged. It should be remembered that the antenna radiator should be at a minimum distance of 20 cm from the human body.**

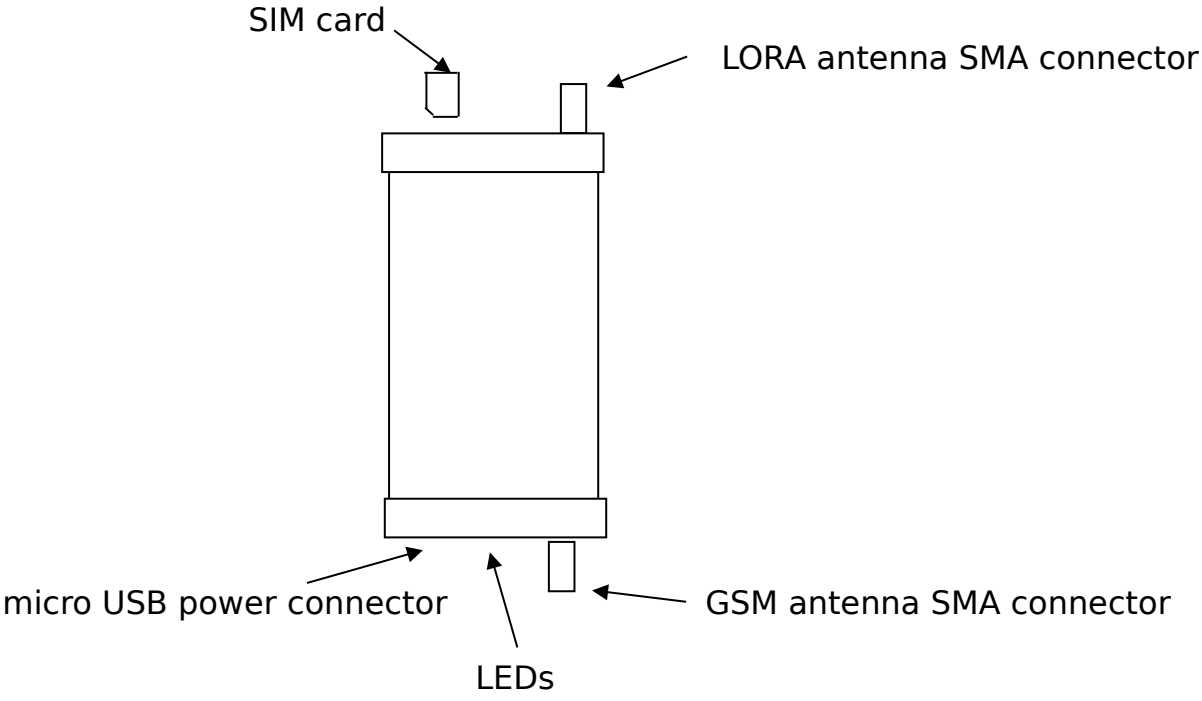



Fig. 1 Top view of the device

## 2.10 LEDs

The table below shows how the red LED states.

| LED state | Operating status of the module |
|---|---|
| Permanently off | The module is in one of the following modes:<br>• Power off mode<br>• SLEEP mode |
| 600 ms off / 600 ms on | The module is in one of the following status:<br>• NO SIM card<br>• SIM PIN<br>• Register network (T<15S)<br>• Register network failure (always) |
| 3 s off / 75 ms on | The module is in one of the following status:<br>• IDLE mode |
| 75 ms off / 75 ms on | The module is in one of the following status:<br>• One or more GPRS contexts activated. |
| Permanently on | The module is in one of the following status:<br>• Voice call |

# 3. MONITOR

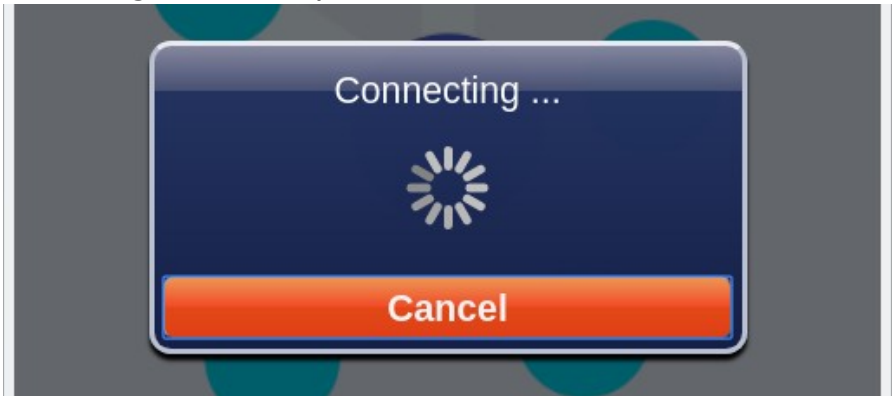
In this mode, **iNode LoRa Monitor** shows from which devices **iNode LoRa** adapter receives broadcast frames. Whether this is in GFSK or in LoRa depends on the adapter configuration. Each type of **iNode LoRa** device has a different icon.

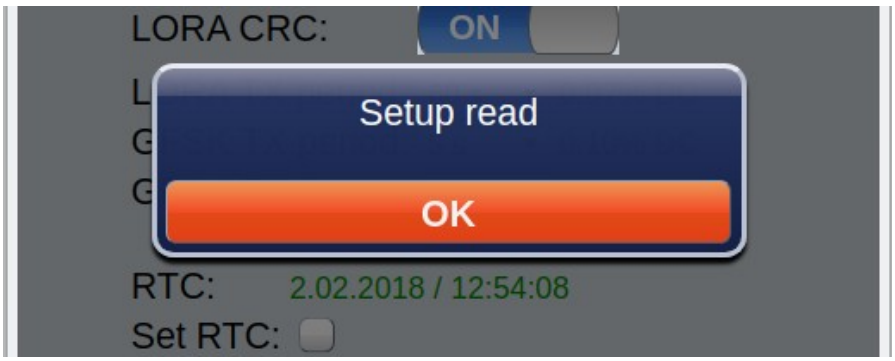

*Scanning effect in LoRa.*


*Scanning effect in GFSK.*

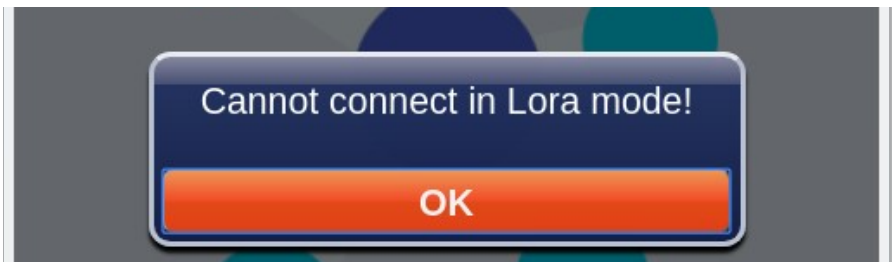
Depending on whether the scan is in GFSK or LoRa, there may be other devices in the list.

The icon  allows establishing connection with the **iNode LoRa** device. This is only possible if the adapter is in GFSK mode and the device you want to connect to also works in this mode. Due to the fact that GFSK modulation enables faster data transmission than LoRa modulation, it was used in **iNode LoRa** sensors to configure and replace firmware.



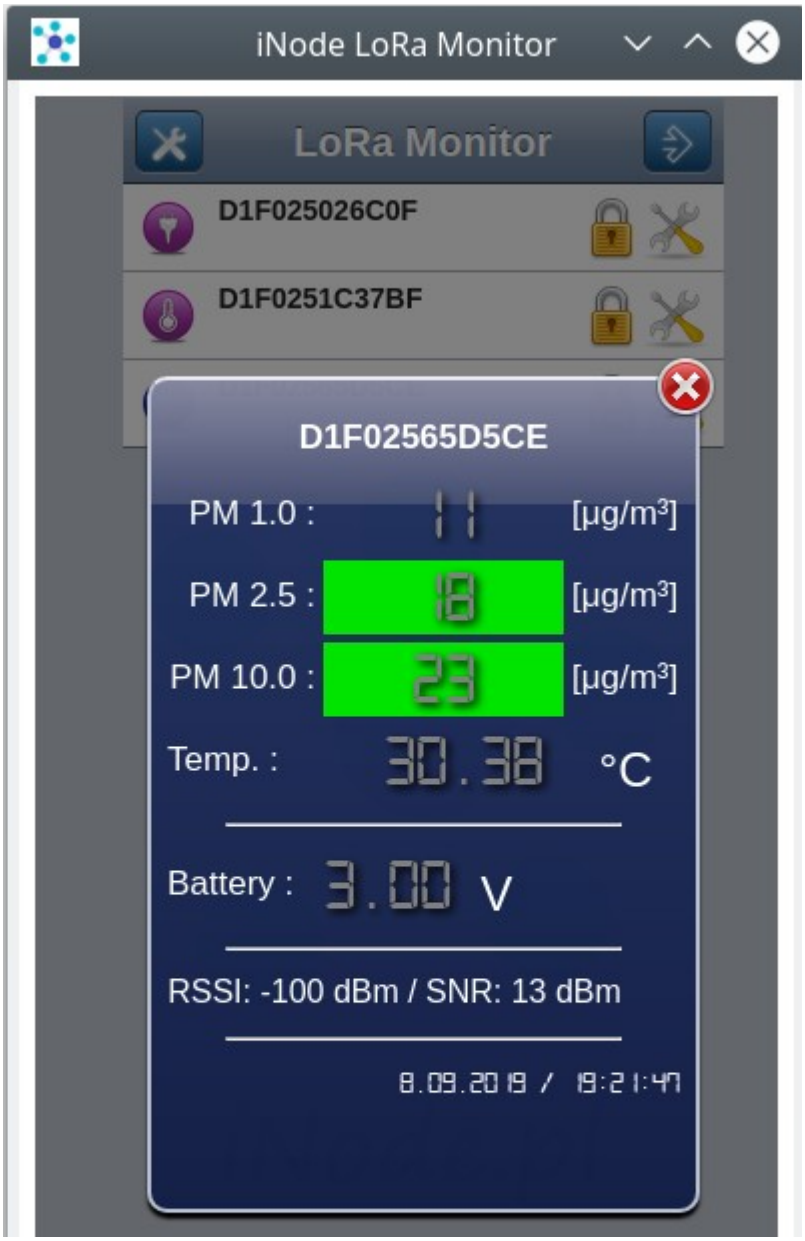

Otherwise, the message *Cannot connect in Lora mode!* will appear.




*Based on Wikipedia about GFSK:*

*GFSK (Gaussian FSK) - a variation of FSK modulation, used for wireless communication within DECT systems, Bluetooth and Z-Wave devices, in which electromagnetic waves in the shape of a Gaussian curve are used. Logical "1" is represented by a positive carrier frequency deviation, and "0" as a negative deviation. In the Bluetooth system, the minimum frequency deviation is 115 kHz. Smoothing of the edges of the impulses is carried out using a Gaussian filter, the effect of which is to reduce the width of the signal spectrum; the next stage is FSK modulation.*

**iNode LoRa Monitor** shows a unique device address on the list of scanned devices. After selecting particular device, a window appears showing the data sent in the broadcast frame received from it.

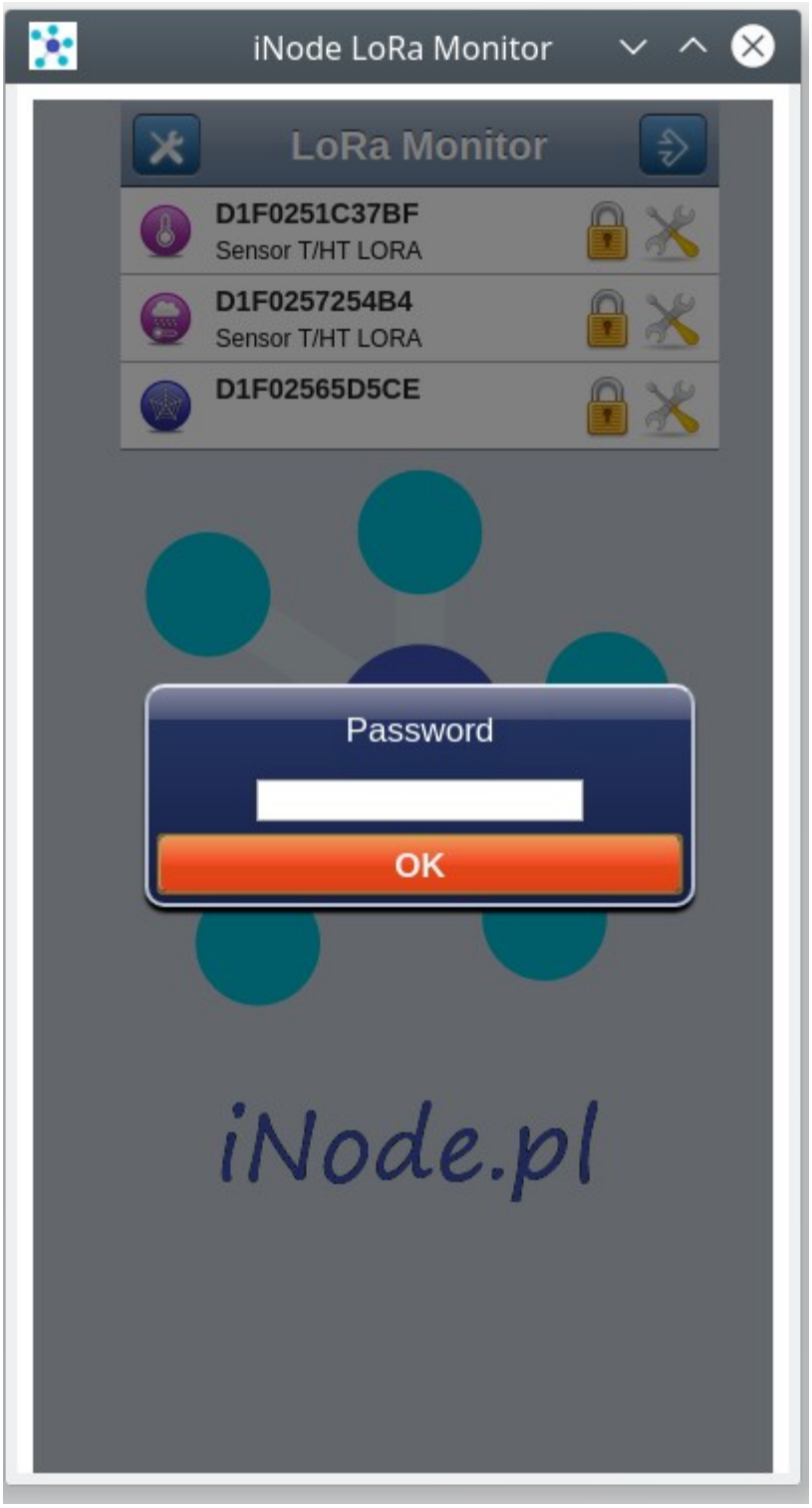



If the **iNode LoRa** device is battery powered, you can see information about the battery voltage. This voltage is measured during transmitting a broadcast frame with LoRa modulation. In idle mode and GFSK one it is higher. The minimum voltage at which **iNode LoRa** devices can work is 1.8V.

In addition, information about the level of the received signal is provided - RSSI and the signal-to-noise ratio - SNR (only in LoRa).

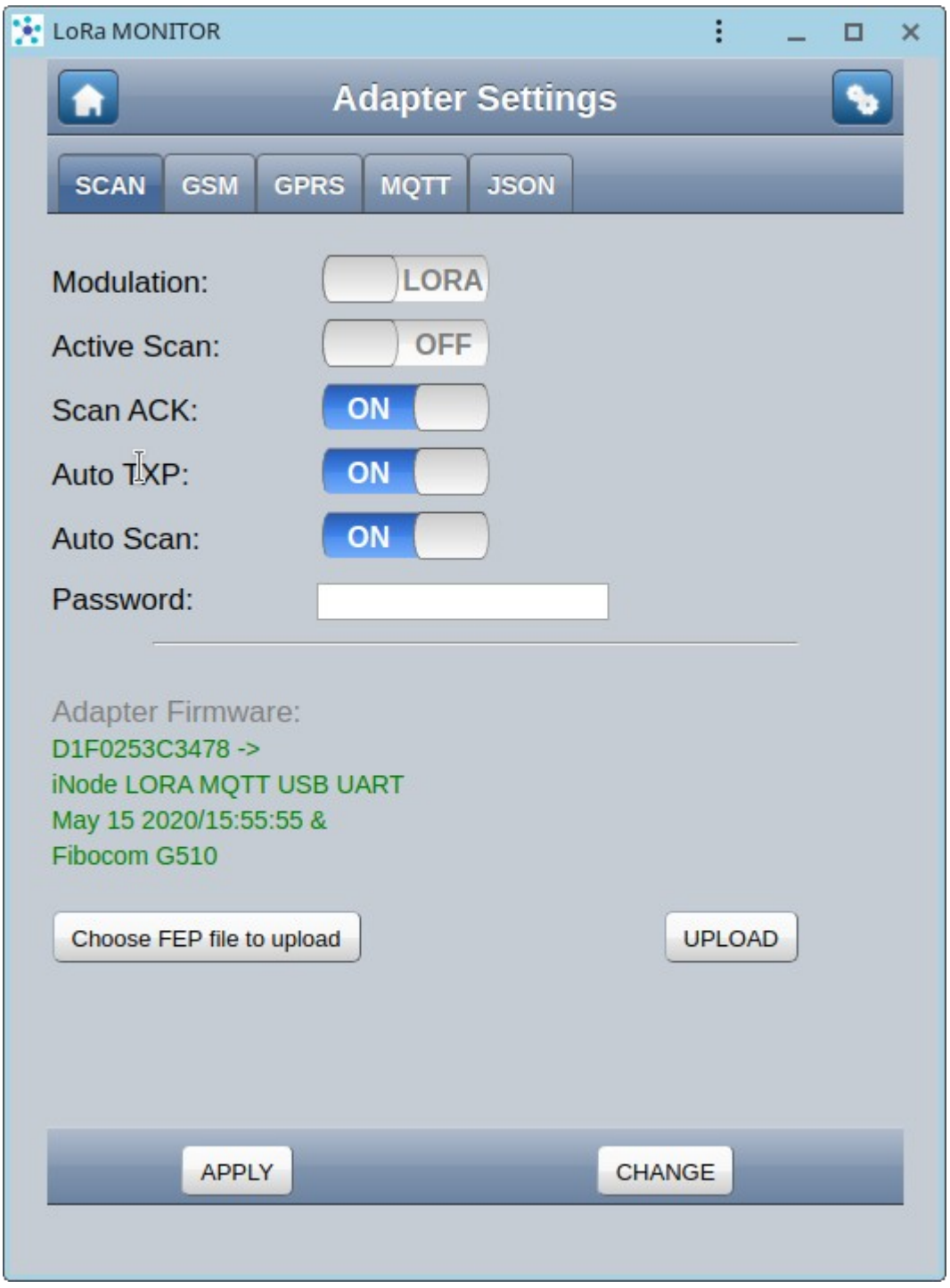
At the very bottom on the right is the date and time of receipt of the last broadcast frame.

The icon  allows you to enter the password necessary to establish a GFSK connection. By default, after the first scan of a device with a given address, it is an empty string. The application remembers entered passwords in the browser database.



# 4. iNode LoRa GSM MQTT adapter settings

To configure the **iNode LoRa GSM MQTT** adapter, go to the icon  This is only possible if the communication with the adapter is correct. After reading the settings from the adapter, the following screen will appear with the ***SCAN*** tab selected by default . The ***APPLY*** button changes settings only until the power is turned off or the adapter is reset. The ***CHANGE*** button changes them permanently and saves them in non-volatile memory. Return to ***MONITOR*** mode is also possible after selecting the icon 



## 4.1 SCAN

This tab allows you to configure the adapter scan parameters and replace the firmware.

### 4.1.1 Modulation

**iNode LoRa GSM MQTT** adapter can receive data by radio using two modulation methods: GFSK or LoRa. GFSK is narrowband modulation and has, with the same transmit power, a smaller range than LoRa. In the case of devices of the **iNode LoRa** family, it is used for configuration and firmware replacement, as it ensures higher speed of data transfer. LoRa is a broadband modulation developed by Semtech. It is characterized by the fact that the receiver can receive a signal that is below the noise level.

### 4.1.2 Active Scan

Depending on the configuration, **iNode LoRa** devices can send, apart from one data packet (so-called broadcast frame) via GFSK, an additional type of packet (so-called active response). The device name is sent in this frame, which the user can change according to his needs. In addition to the unique device address, its name will appear in the **iNode LoRa Monitor** application.

### 4.1.3 Scan ACK

After enabling this mode of operation, if the adapter works in LoRa, it sends automatically after receiving the broadcast frame, confirmation of its receipt to the sender.

### 4.1.4 Auto TXP

After activating this mode of operation, if the adapter works in LoRa, it sends automatically after receiving the broadcast frame, confirmation of its receipt to the sender so that it can adjust its transmission power to the ambient conditions.

### 4.1.5 Auto Scan

After activating this mode of operation and saving it in the adapter, if the adapter is connected to the USB connector, it will immediately go into scan mode. To avoid buffer overflow in the adapter when no application is receiving data from it, USB data transfer is disabled by default. To activate them you must either configure the COM port parameters or send some data to the adapter.

### 4.1.6 Password

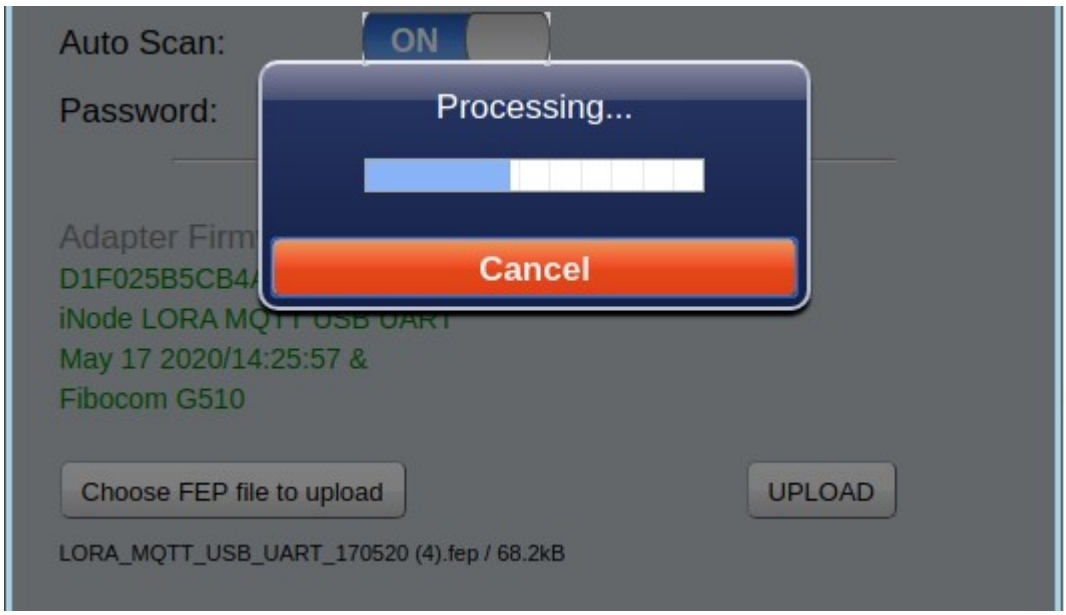
In this window, you can enter a password to limit access to the adapter configuration. At this time this functionality is not active.

### 4.1.7 Firmware Adapter

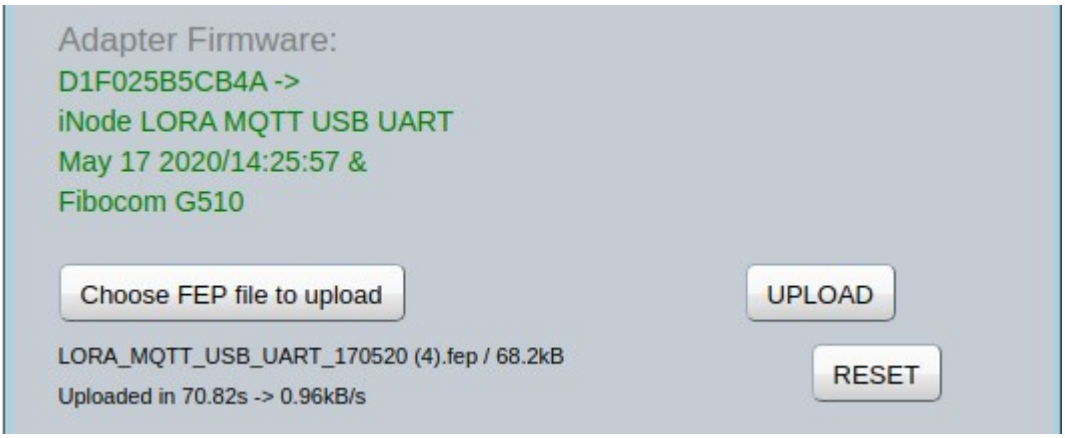
This part of the tab displays information about the firmware in the adapter and its MAC address. After pressing the ***Choose FEP file to upload*** button , the system browser window will appear for choosing a firmware file. Files with firmware for **iNode LoRa** devices have the extension .fep and contain information for which device they are intended. Therefore, it is not possible to upload to the device firmware intended for another.

When you press the ***UPLOAD*** button, a window will appear showing the progress of sending the firmware to the device.

Make sure that the device does not have a SIM card at the time, because the power consumption of the modem in it may be too high for the USB port to which **iNode LoRa GSM MQTT** is connected. The result will be a power cut when replacing the firmware, which may result in a device failure.




When the firmware is sent, information about the data transfer speed and the ***RESET*** button will appear.

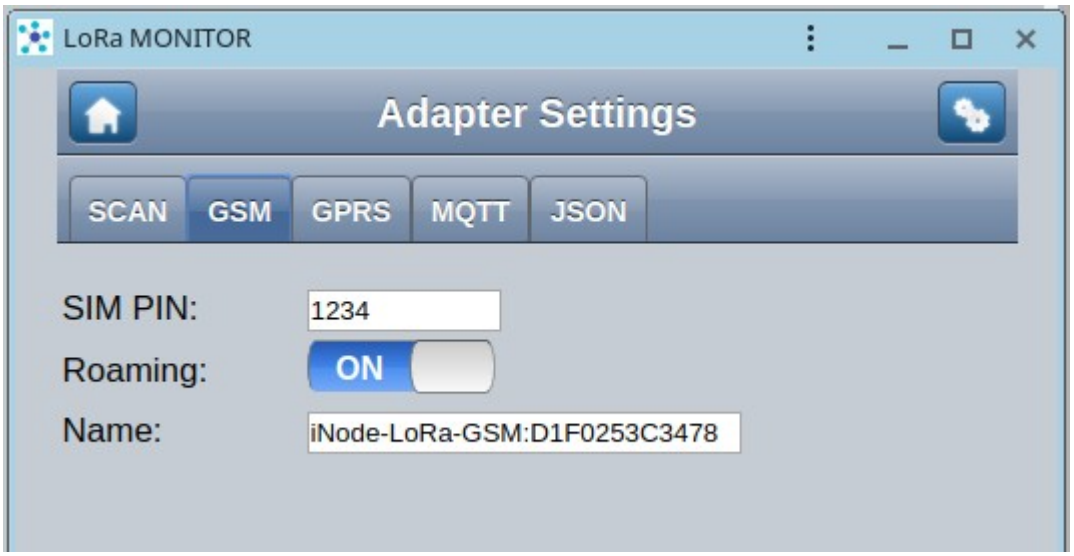


After pressing the ***RESET*** button the firmware will be replaced, the device will restart and be connected again to the **iNode LoRa Monitor** application.

In the case of the **iNode Lora GSM MQTT** adapter are available additional tabs.

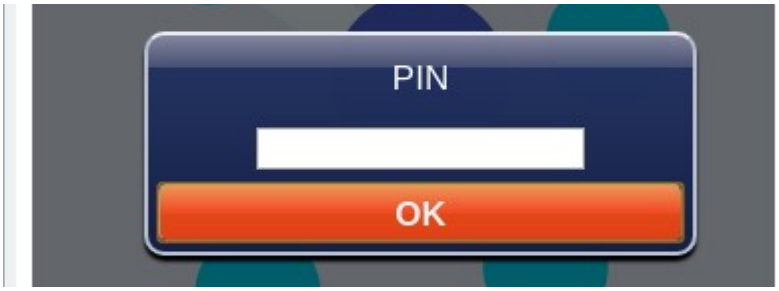
## 4.2 GSM

This tab allows you to configure the parameters associated with the SIM card.




### 4.2.1 SIM PIN

Here we provide the PIN number to the SIM card located in the device. Its length is 4 digits. The same PIN must be entered to access device settings from the **iNode LoRa Monitor** application.




The application remembers the provided PIN number in the browser.

### 4.2.2 Roaming

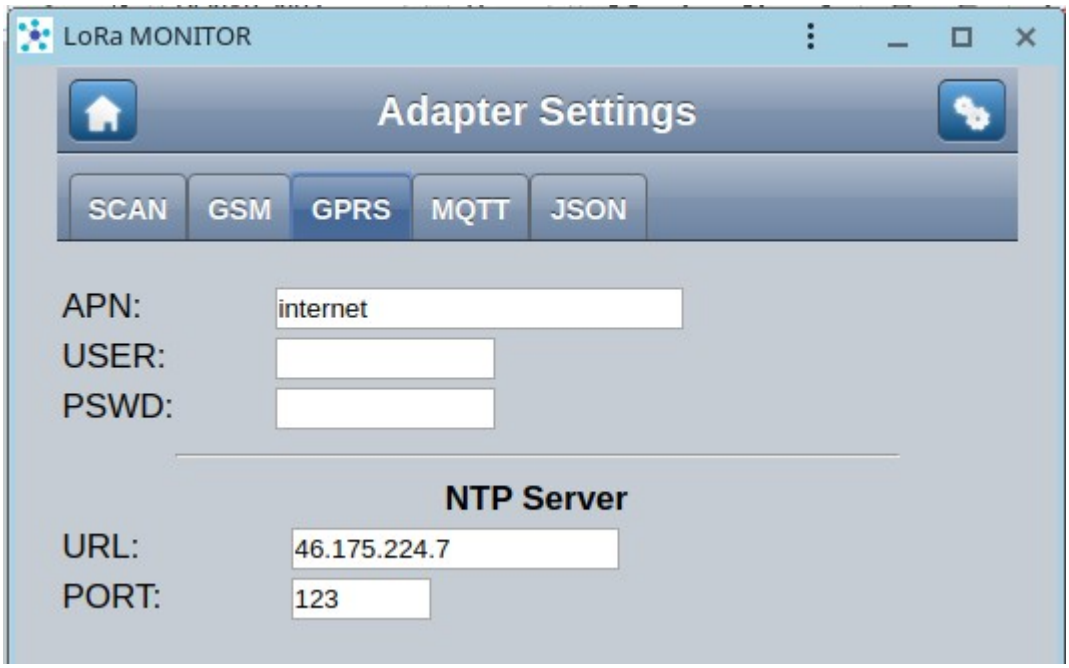
If the SIM card is to work in domestic or foreign roaming, select this option.

### 4.2.3 Name

Here we provide the name of the device which is forwarded to the MQTT server.

## 4.3 GPRS

This tab allows you to configure the GPRS connection parameters.




### 4.3.1 APN

Enter the APN name here. The maximum length is 16 characters.

### 4.3.2 USER

Here we provide the username appropriate for a given APN. The maximum length is 16 characters.

### 4.3.3 PSWD

Here we provide the password appropriate for the given user. The maximum length is 16 characters.

### 4.3.4 NTP Server - URL

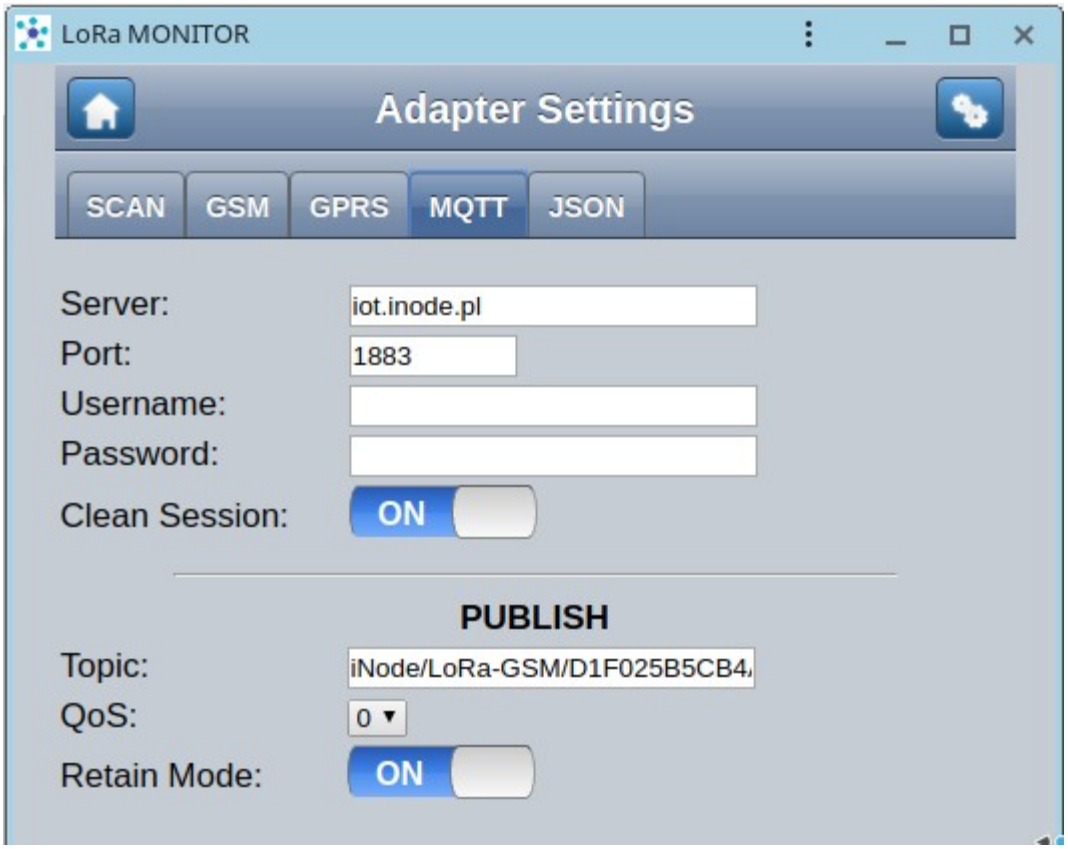
Here we provide the URL of the NTP server in numerical form. The maximum length is 32 characters.

### 4.3.5 NTP Server - PORT

Here we provide the NTP server port number in the range 0 to 65535.

## 4.4 MQTT

This tab allows you to configure the parameters of the MQTT server to which the device sends data.




### 4.4.1 Server

Enter the address of the MQTT server that is to receive data from the device. The maximum length is 32 characters.

### 4.4.2 Port

Enter the MQTT server port here to receive data from the device. It should be in the range 0 to 65535.

### 4.4.3 USER

Here we provide the username for access to the MQTT server. The maximum length is 16 characters.

### 4.4.4 PSWD

Here we provide the password appropriate for access to the MQTT server. The maximum length is 16 characters.

### 4.4.5 Clean Session

When the ***MQTT Clean Session*** flag is enabled, the client does not want a persistent session. If the client disconnects for any reason, all information and messages in the queue from the previous persistent session are lost.

### 4.4.6 PUBLISH - Topic

Enter here Topic to which statistical data is sent via **iNode LoRa GSM MQTT**. Data from LoRa sensors are published under the same Topic at the end of which the sensor's MAC is added after the / sign.

### 4.4.7 PUBLISH - QoS

The meaning of ***MQTT PUBLISH QoS*** is as follows:

- QoS 0 - the client will not receive any confirmation from the server. Similarly, the message delivered to the client from the server does not have to be confirmed. This is the fastest way to post and receive messages, but also the one where you will most likely lose messages.
- QoS 1 - the client will receive a confirmation message from the server after it has been published. If the expected confirmation is not received within the specified time, the customer must retry the message. The message received by the client must also be confirmed in time, otherwise the server will deliver the message again.

### 4.4.8 PUBLISH – Retain Mode

If it is ON - then the last message sent is remembered by the MQTT server.

Default device settings enable cooperation with the MQTT iNode server - iot.inode.pl

## 4.5 JSON

This tab allows you to configure the parameters of the MQTT server to which the device sends data. The data received from the **iNode LoRA** sensors are sent to the MQTT server as soon as they are received.


### 4.5.1 RSSI

Threshold level; further filters only take into account devices from which the received signal level is higher than that set here. The value -128 means any signal level.

### 4.5.2 MAC - MASK

MAC address mask.

### 4.5.3 MAC - PATTERN

The MAC address with which the received MAC is compared after the AND operation with the MAC mask.

### 4.5.4 MANUF - MASK

Manufacturer Specific Data mask.

### 4.5.5 MANUF - PATTERN

Manufacturer Specific Data with which the received Manufacturer Specific Data is compared after the AND operation with the Manufacturer Specific Data mask.

### 4.5.6 Period

Time period for sending statistical data by iNode LoRa GSM to the MQTT server.

### 4.5.7 Encryption

If it is ON - the data sent to the MQTT server is encrypted.

### 4.5.8 KEY

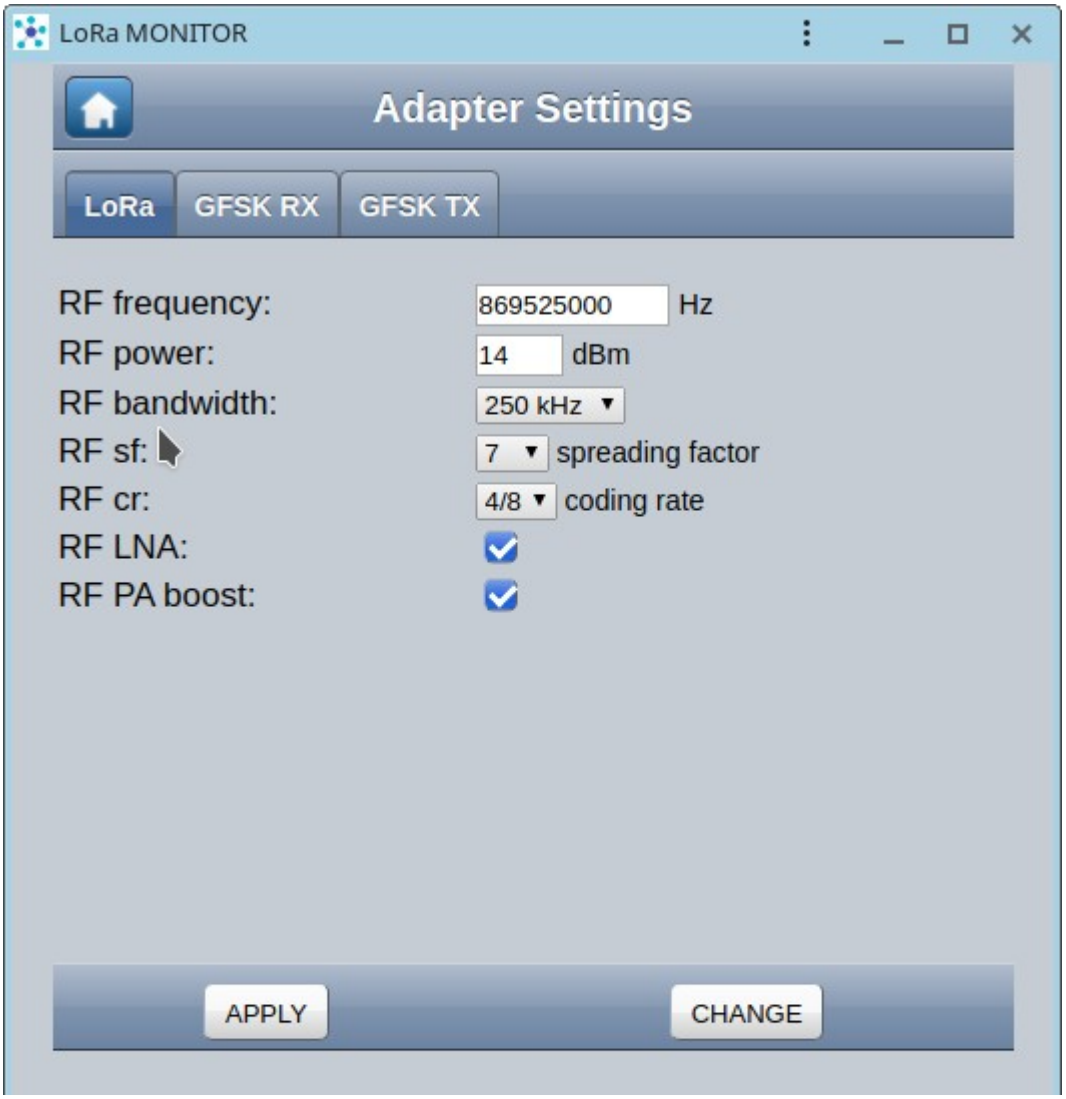
Master key for encrypting data. **iNode LoRa GSM MQTT** encrypts the sent JSON data using a different temporary key each time, which is encrypted with the master key and placed at the beginning of the JSON data.

The key length is a maximum of 16 characters. The same key must be later entered in the **iNode MQTT Monitor** application so that it can decode the data. During the firmware exchange operation , when the default settings of the device are changed - a random one is created for a new key.

After selecting the button  the **iNode LoRa Monitor** application will allow you to configure the RF (radio) parameters of the device.

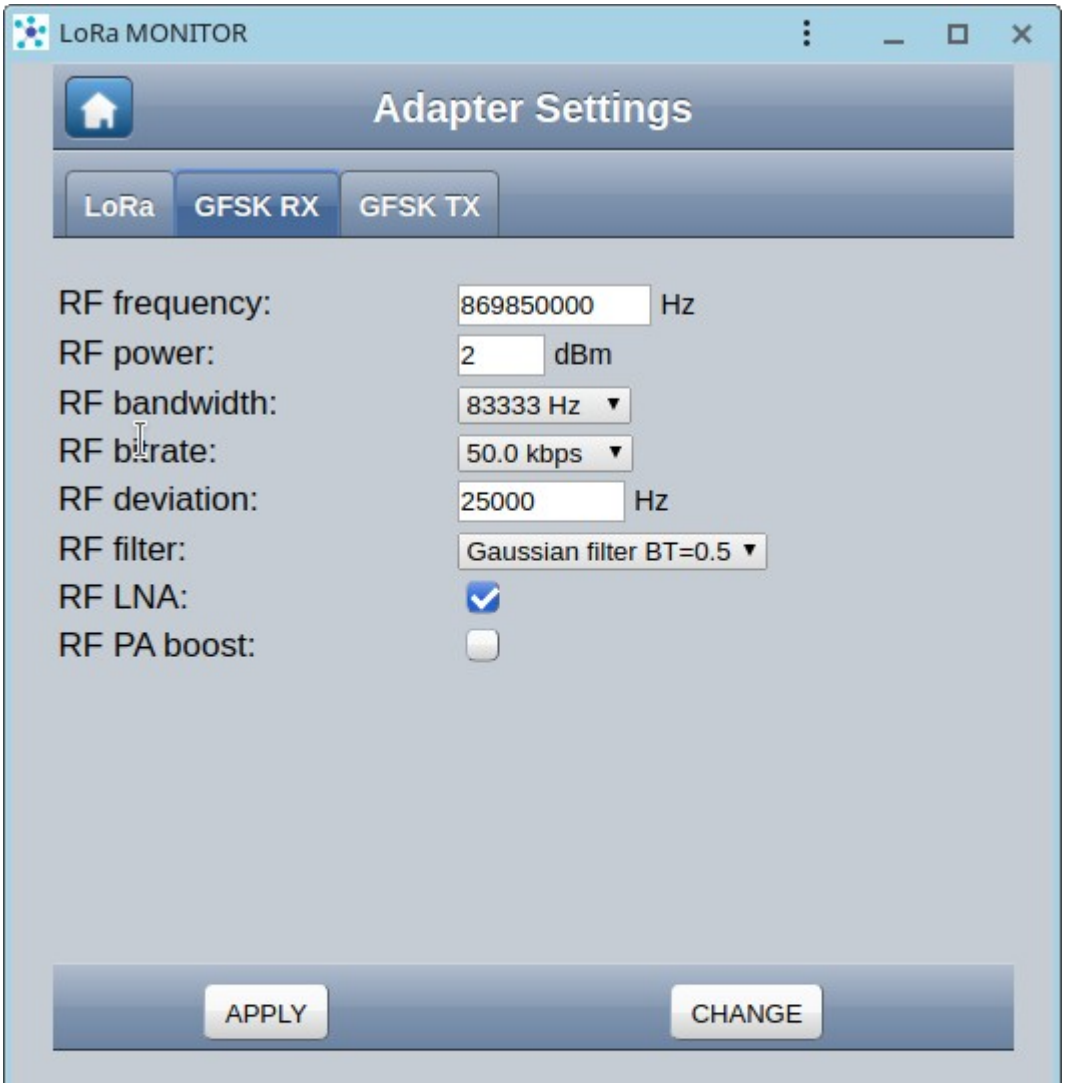
## 4.6 LoRa

This tab allows you to change the adapter LoRa modulation parameters. Please note that these parameters must be the same in the sending **iNode LoRa** device, otherwise the adapter will not receive any data from it. Below all parameters information is displayed, what is the maximum permissible value of DC factor in a given frequency band, and what is obtained by the device - LORA TX DC. This information is only helpful and the user should confirm it with the regulator. The maximum output power allowed in Europe by ETSI is +14 dBm.



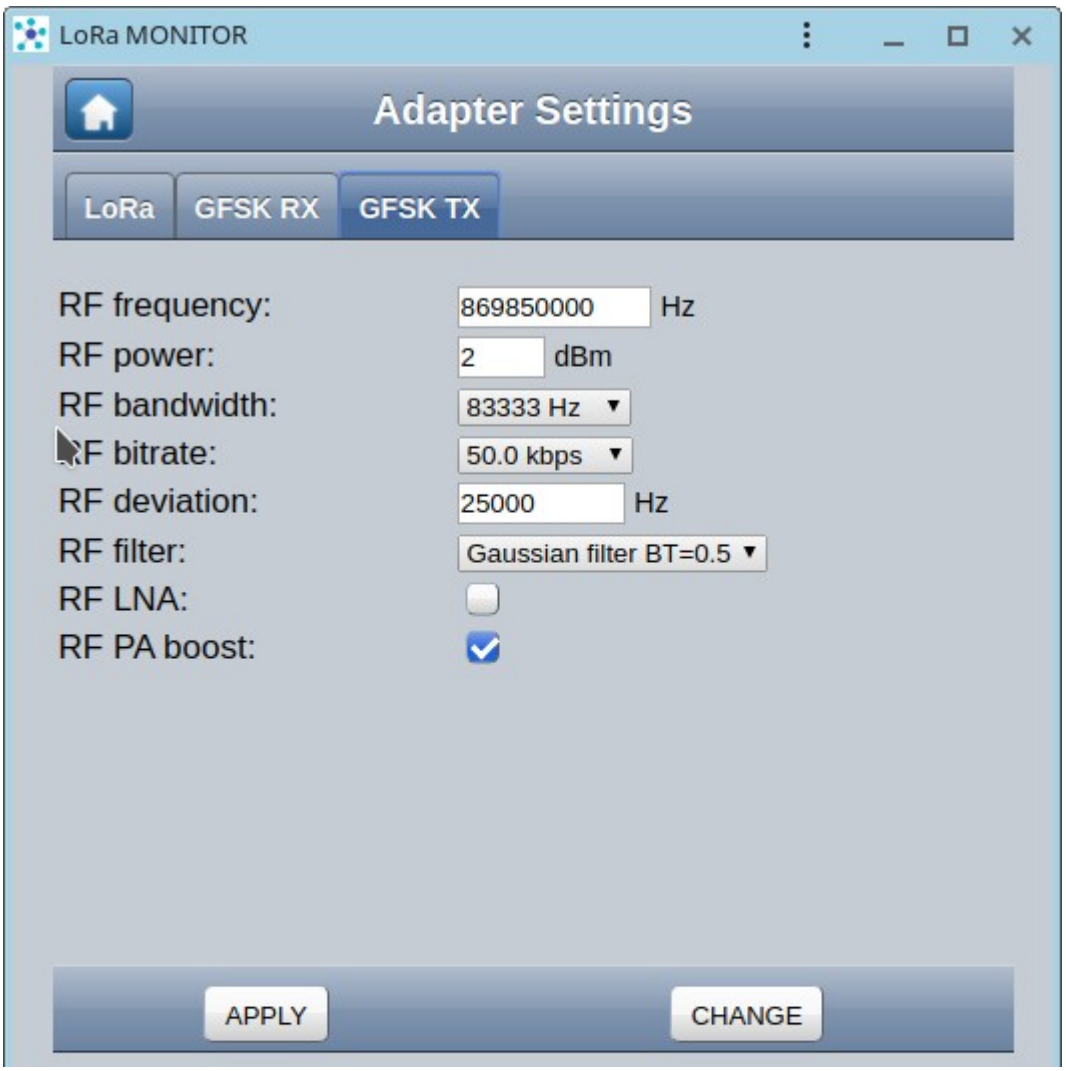
## 4.7 GFSK RX

This tab allows you to change the GFSK modulation parameters of the device in RX mode, i.e. receiving data. Please note that these parameters must be the same (GFSK TX) in **iNode LoRa** devices, otherwise the adapter will not receive any data from them.



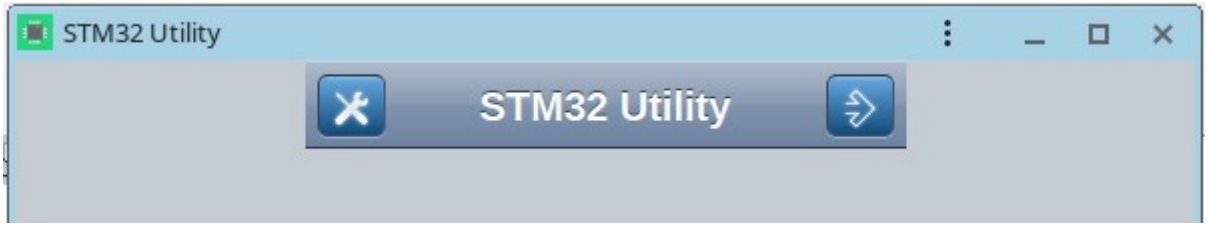
## 4.8 GFSK TX

This tab allows you to change the GFSK modulation parameters of the device in TX mode, i.e. sending data. Please note that these parameters must be the same (GFSK RX) in **iNode LoRa** devices, otherwise they will not receive any data from the **iNode LoRa GSM MQTT**. Below all parameters information is displayed, what is the maximum permissible value of DC coefficient in a given frequency band, and what is obtained by the device - GFSK TX DC. This information is only helpful and the user should confirm it with the regulator. The maximum output power allowed in Europe by ETSI is +14 dBm.

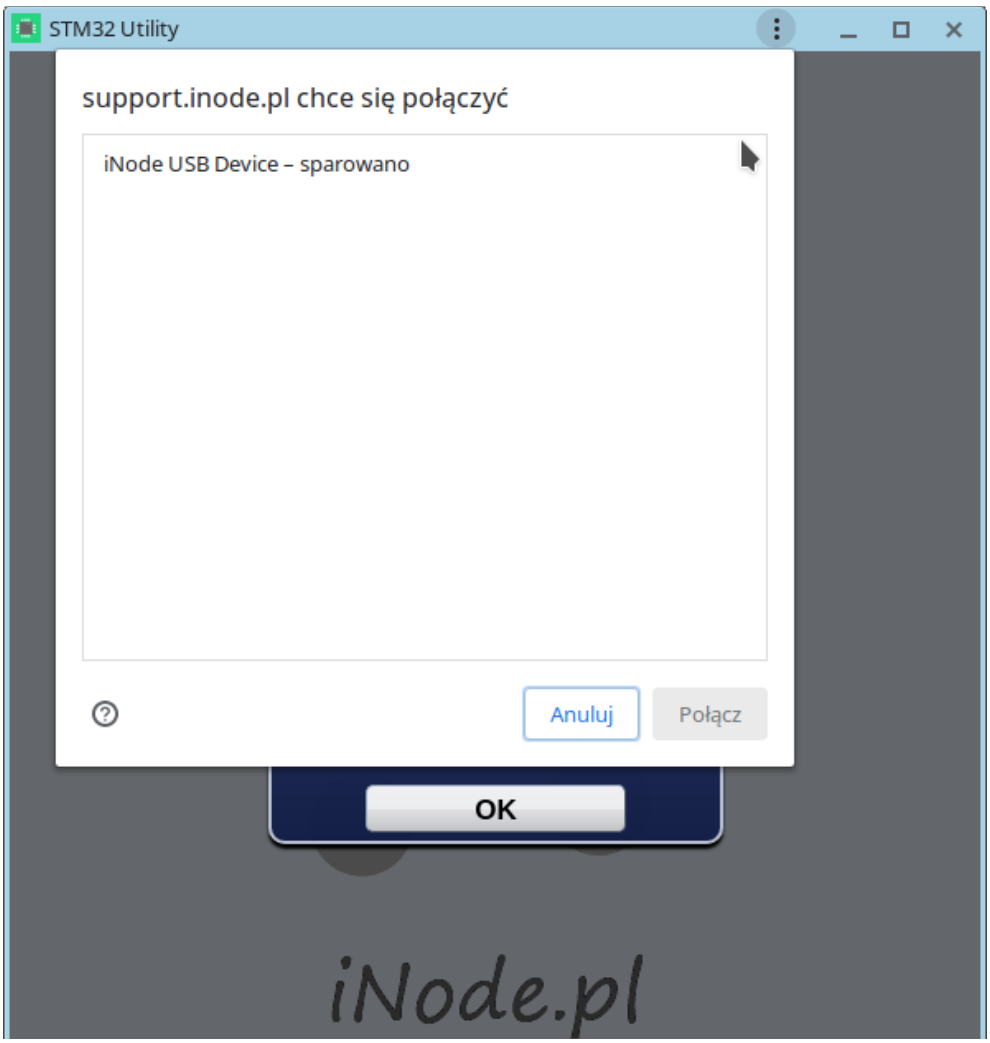


# 5. STM32 Utility

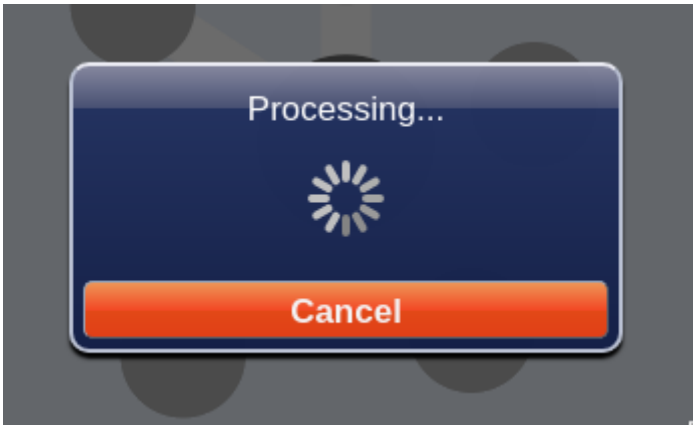
The iNode STM32 Utility application is used to exchange firmware in **iNode** devices with a USB port supported by the STM32 chip. It must be running in Chrome, because only then you can use the USB adapter WebUSB functionality. Its installation is similar to the installation of the iNode Lora Monitor application.



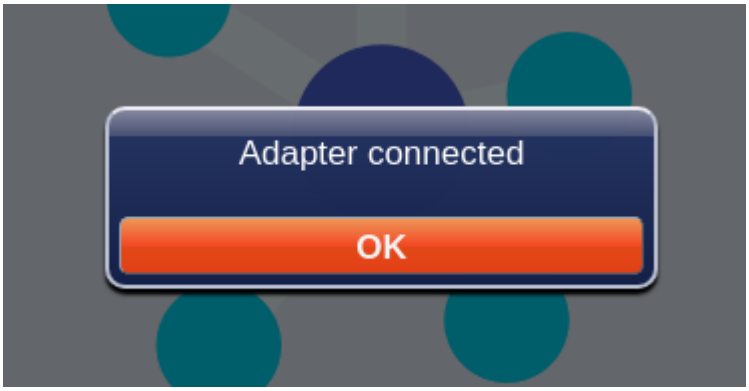

After selecting the icon,  we can choose the connection method with the iNode USB adapter.




After selecting the adapter type - in this case it must be STM and USB port - the application will connect with the USB adapter.


The message ***Adapter connected*** will appear.



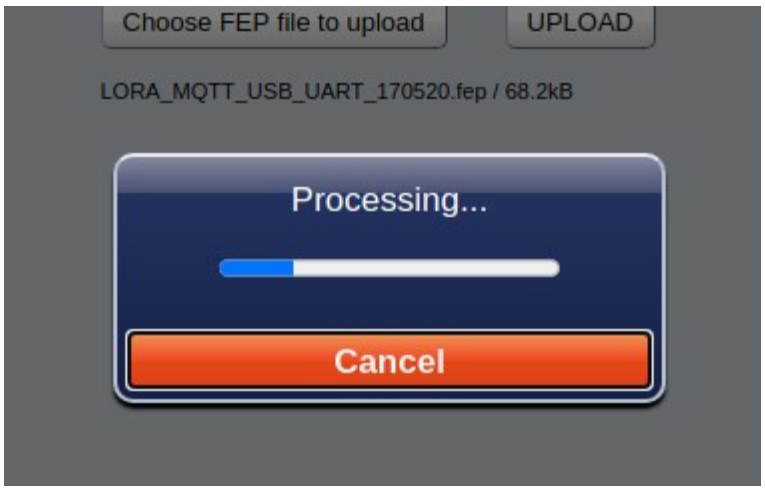

To configure the **iNode LoRa GSM MQTT** adapter, go to the icon 

This is only possible if the communication with the adapter is correct. After reading the settings from the adapter, the following screen will appear with the ***FRM*** tab selected by default. Return to the initial screen is possible after selecting the icon 

The ***FRM*** tab provides information about the firmware in STM32 and allows it to be replaced.

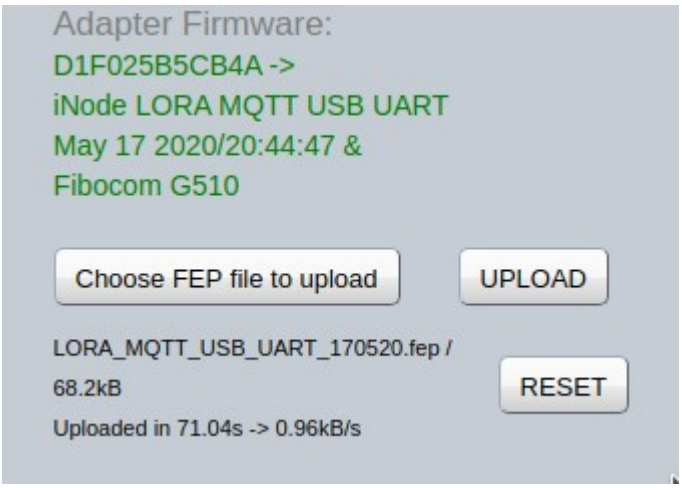

The ***Adapter Firmware*** part of the tab displays information about the firmware in the adapter and its MAC address. After pressing the ***Choose FEP file to upload*** button, the system browser window will appear for choosing a firmware file. Files with firmware for **iNode LoRa** devices have the extension .fep and contain information for which device they are intended. Therefore, it is not possible to upload to the device firmware intended for another.

When you press the ***UPLOAD*** button, a window will appear showing the progress of sending the firmware to the device.



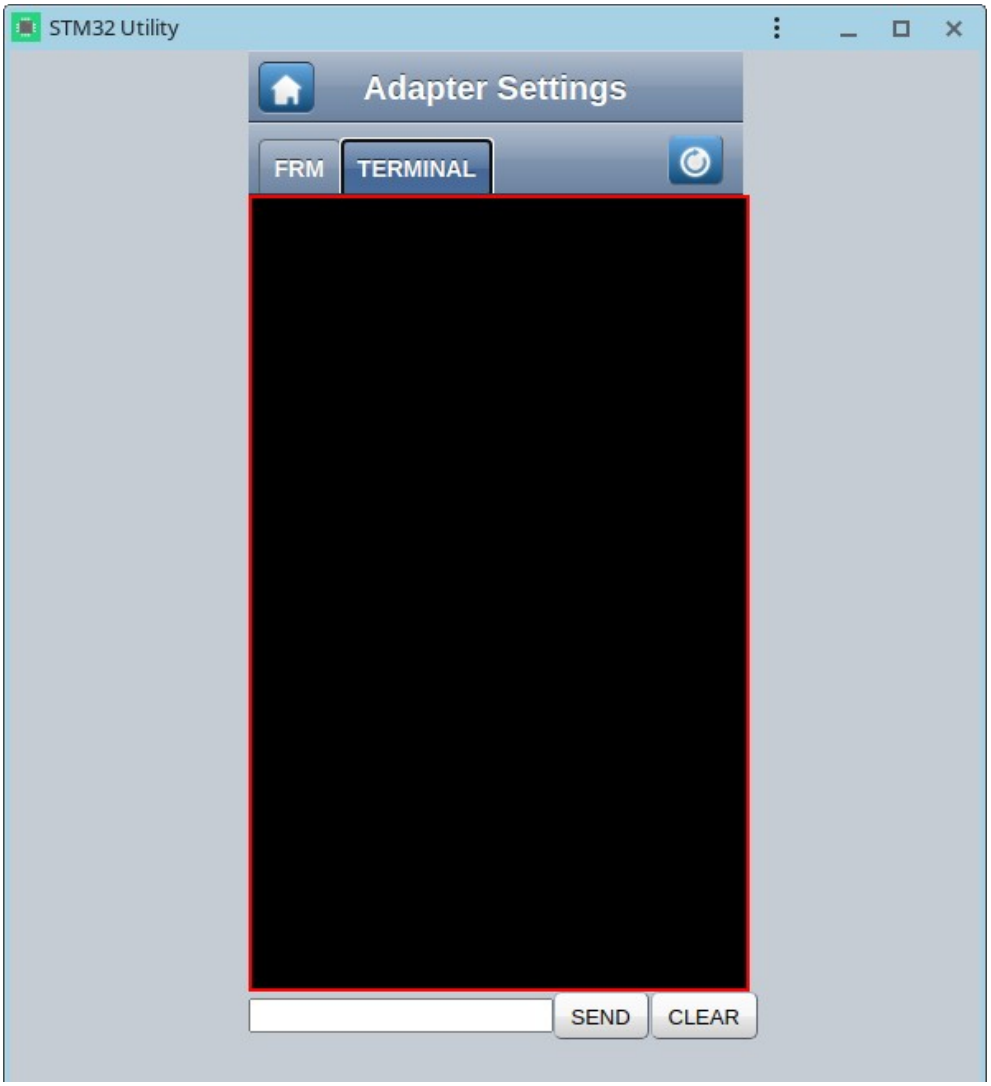

Make sure that the device does not have a SIM card at the time, because the power consumption of the modem in it may be too high for the USB port to which **iNode LoRa GSM MQTT** is connected. The result will be a power cut when replacing the firmware, which may result in a device failure.

After sending the firmware, information about the data transfer speed and the ***RESET*** button will appear.




After pressing the ***RESET*** button the firmware will be replaced, the device will restart and be connected again to the ***iNode STM32 Utility*** application.

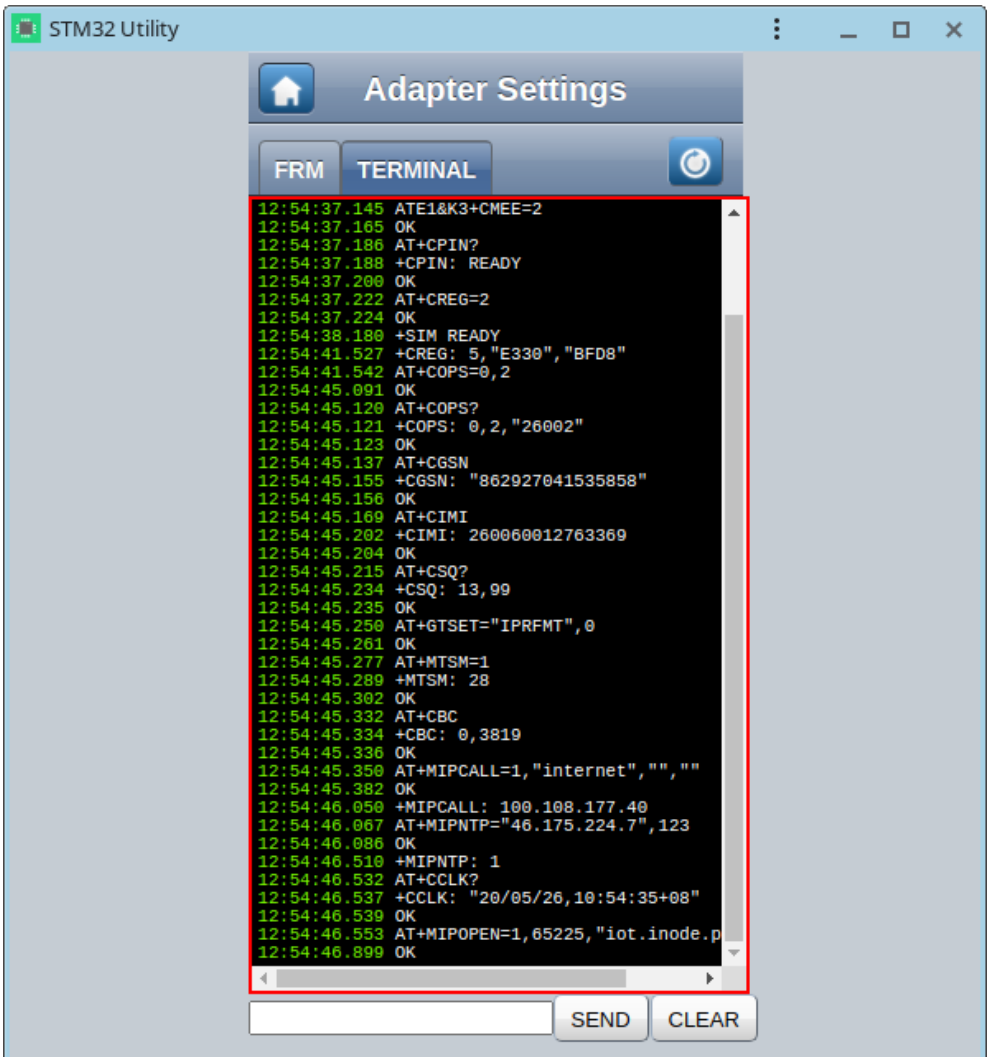
The ***TERMINAL*** tab enables communication with the Fibocom G510 modem located in the device. The ***SEND*** and ***CLEAR*** buttons are used for this. ***SEND*** sends a text string from the left pane. ***CLEAR*** deletes the contents of this window.




After connecting the i**Node LoRa GSM MQTT** to the computer, the device does not communicate with the modem. It starts only after the modem has been reset with the button 

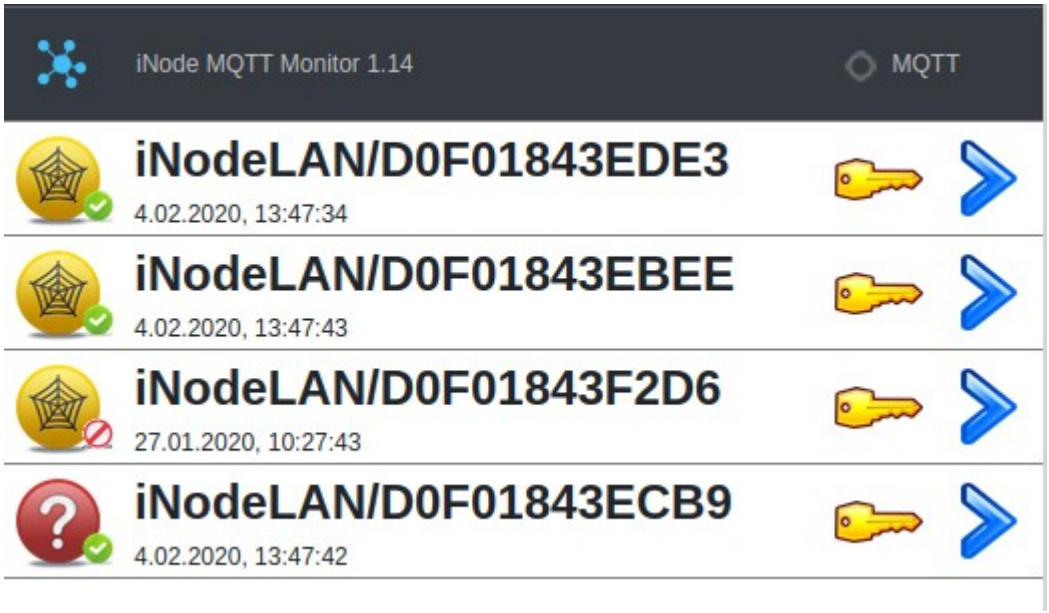
A window then appears a sequence of AT commands sent by the device and responses from the modem. Thanks to this, when something is not working properly, you can easily figure out which AT command is causing the problem.

Since the modem during operation consumes a significant current, exceeding the performance of a typical USB port, it should be ensured that **iNode LoRa GSM MQTT** was connected to a USB hub with an additional power supply, and not directly to the PC.



# 6. MQTT MONITOR

The iNode MQTT MONITOR application allows you to test communication between the device and the MQTT or HTTP/POST server . The **iNode MQTT Monitor** application is dedicated to the Google Chrome browser and works on Android, Windows, Linux operating systems, etc. After loading the application, it can be installed for easier launch later. An application icon will appear on the main screen.

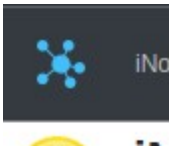



After starting the application, it shows devices that send data to the MQTT server iot.inode.pl. This is a free MQTT test server for users of the iNode products.

## Important !

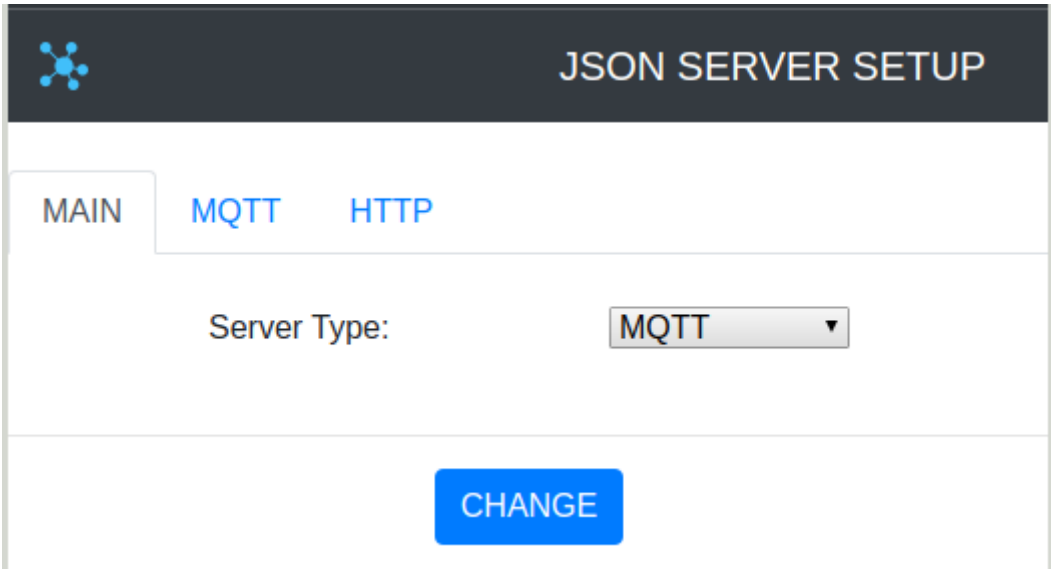
ELSAT s.c. does not guarantee that the MQTT iot.inode.pl server will be available in the future and under what conditions. The user must be aware that data sent to this server may be received by others. For privacy, you should ensure that send on this server data to be encrypted - this is the default option in the **iNode Lora GSM MQTT** device. The default password for encrypting them is different and randomly created on each device. The data on the server are not archived in any way, but they are publicly available, which results from the specifics of the MQTT server operation if access to it is not restricted by means of a username and password. ELSAT s.c. is not responsible for the content of this data in any way and does not interfere in any way – moderates it.

Configuration of the **iNode MQTT Monitor** application is done by clicking on the image in the upper left corner of the screen:

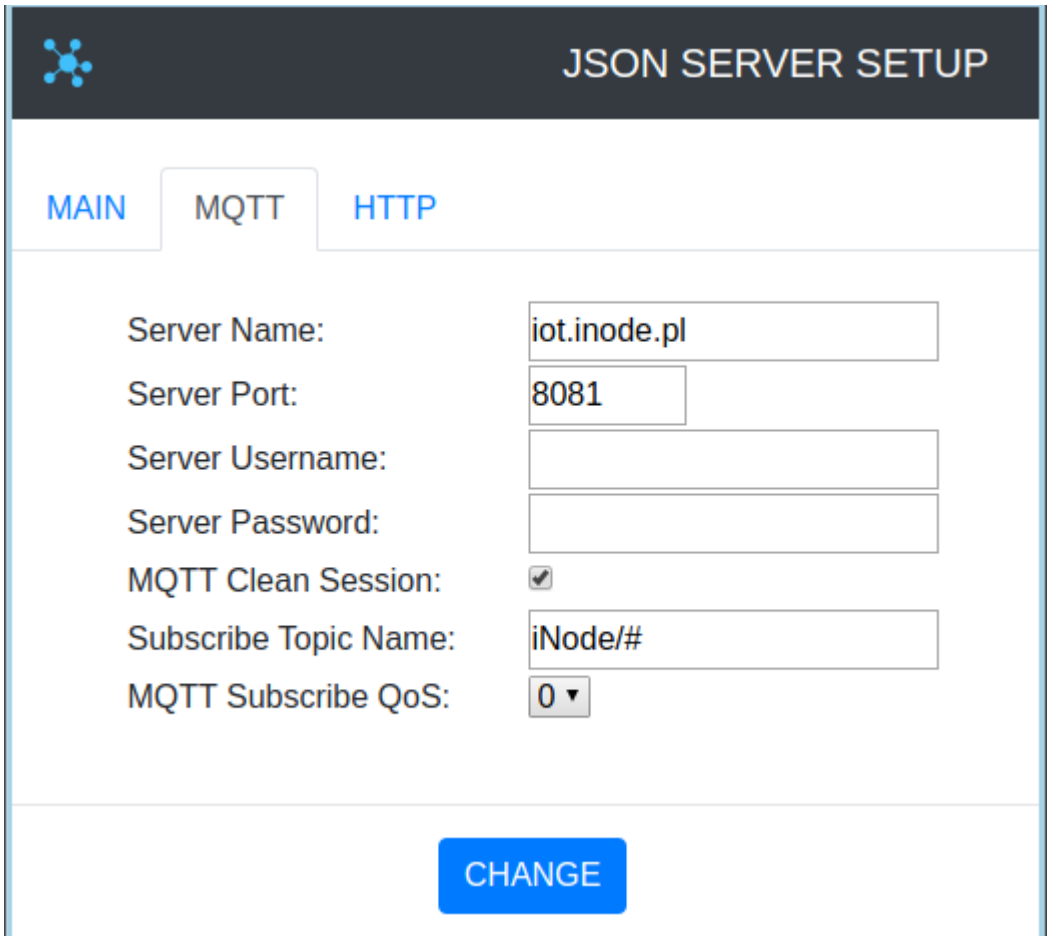


The following application screen will appear - **JSON SERVER SETUP**:

The ***MAIN*** tab allows you to select the type of server with which the application is to work. It can be HTTP, MQTT, USB or BLUETOOTH. The latter option is available from Google Chrome 79, however, so far it works only under Android. You may need to enable in **chrome://flags/#enable-experimental-web-platform-features** for USB or BLUETOOTH.

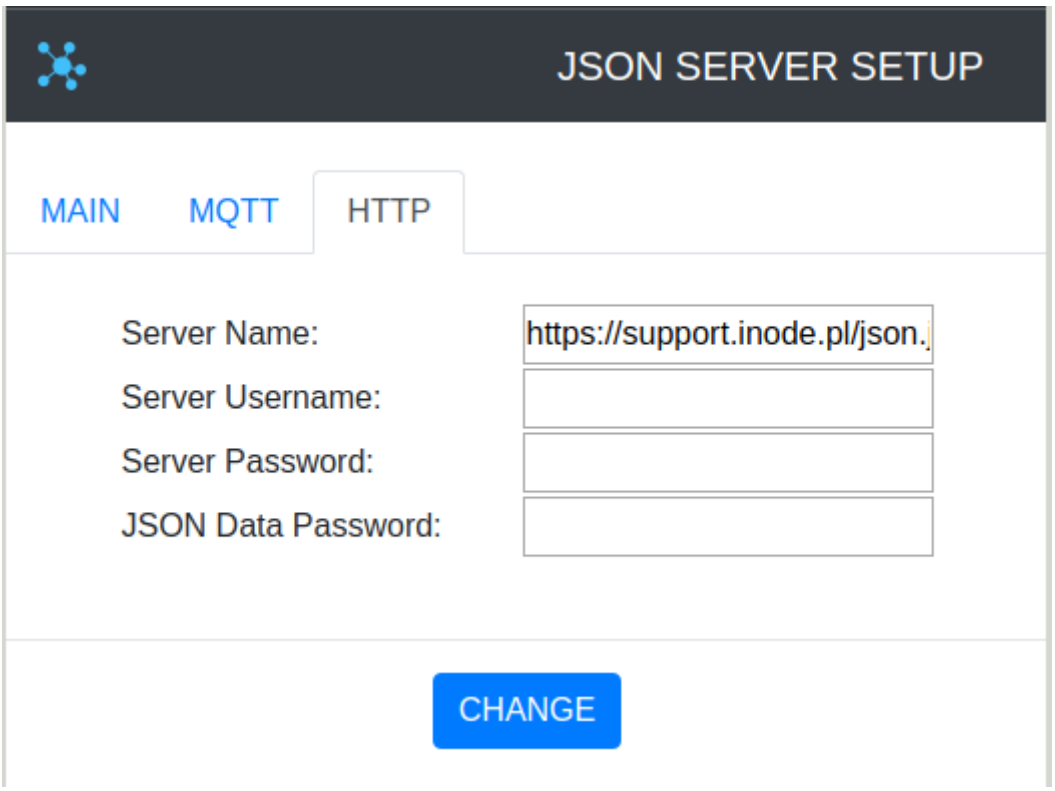



The ***MQTT*** tab allows you to enter the parameters of the MQTT server.



- ***Server Name*** – server name
- ***Server Port*** – the port at which the WebSocket service of the MQTT server is available
- ***Server Username*** – username if access to the MQTT server is restricted
- ***Server Password*** – password to access the MQTT server
- ***MQTT Clean Session*** - when the ***MQTT Clean Session*** flag is set, the client does not want a persistent session. If the client disconnects for any reason, all information and messages in the queue from the previous persistent session are lost.
- ***Subscribe Topic Name*** – it must be the same value as in the **iNode LoRa GSM MQTT** settings in the **PUBLISH – Topic** field or its fragment.
- ***MQTT Subscribe QoS:***
  - ***QoS 0*** - the client will not receive any confirmation from the server. Similarly, the message delivered to the client from the server does not have to be confirmed. This is the fastest way to post and receive messages, but also the one where you will most likely lose messages.
  - ***QoS 1*** - the client will receive a confirmation message from the server after it has been published. If the expected confirmation is not received within the specified time, the customer must retry the message. The message received by the client must also be confirmed in time, otherwise the server will deliver the message again.

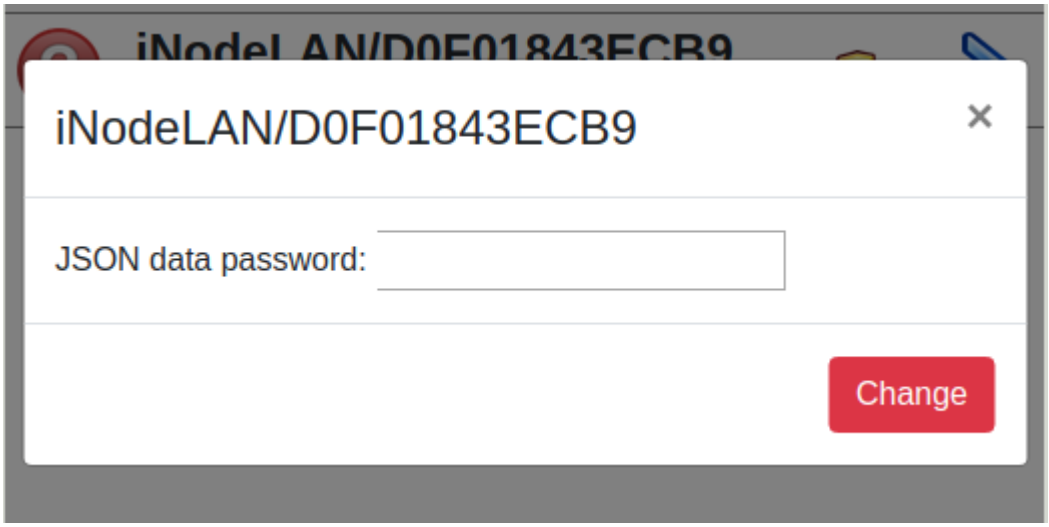
The ***HTTP*** tab allows you to specify HTTP server parameters.

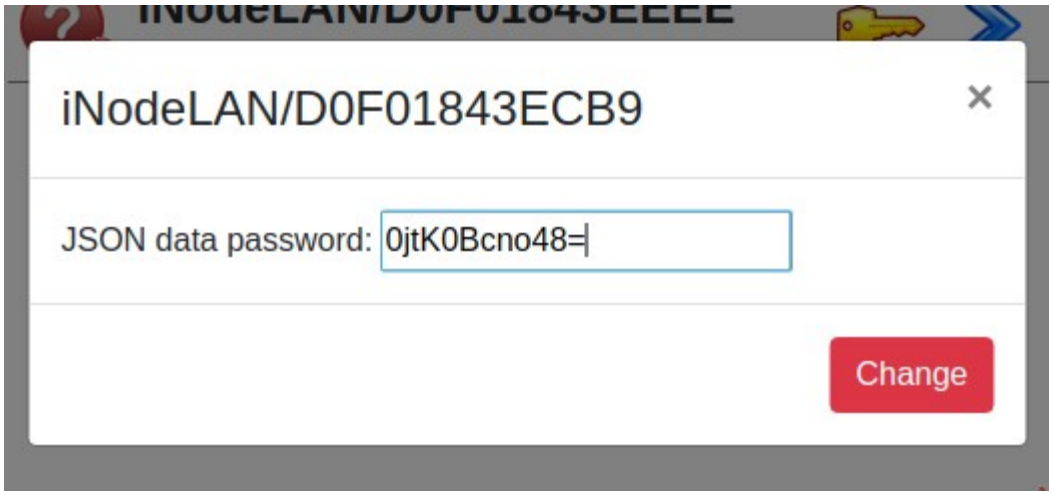



- ***Server Name*** – a full url containing the server name and path to the file with the given JSON
- ***Server Port*** – the port at which the HTTP server service is available
- ***Server Username*** – username if access to the HTTP server is restricted. Basic authorization type

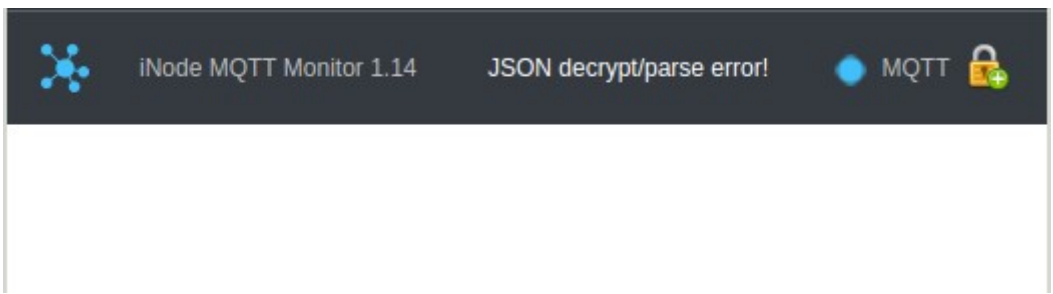
- ***Server Password*** – password to access the HTTP server

If **iNode LoRa GSM MQTT** sends encrypted JSON data, then after selecting the picture with the key, enter the password to decode them and press the ***CHANGE*** button . It must be the same password as in the ***JSON*** tab in the ***KEY*** field.

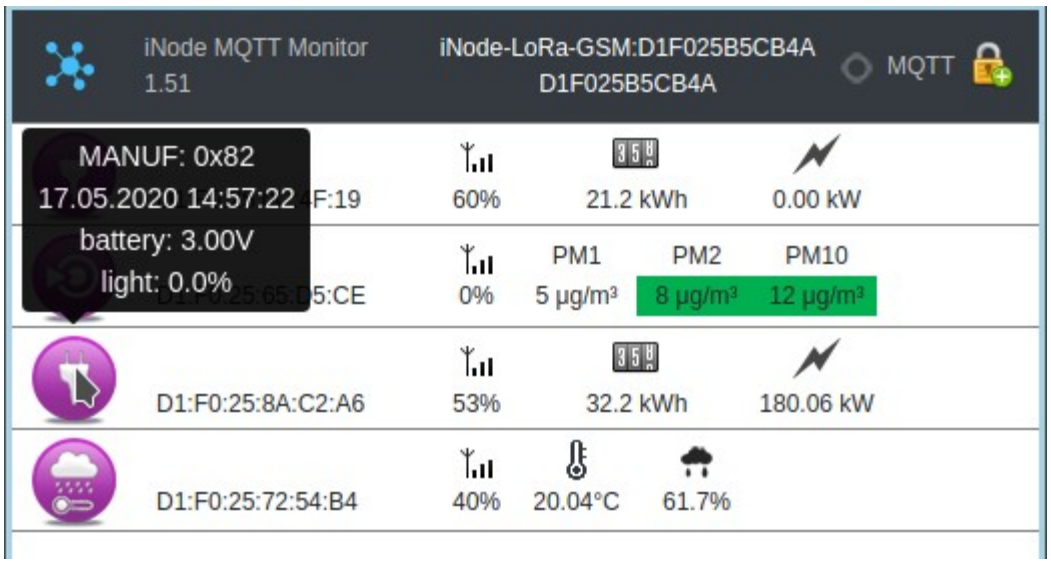



If the password is unset or wrong, after selecting the blue right arrow an error message will appear - ***JSON decrypt/parse error***. The fact that the data is encrypted is shown by a picture of the padlock in the upper right corner of the screen.



If the password was entered correctly, the application will display information about the devices from which they are sent by the given **iNode LoRa GSM MQTT**. By hovering the mouse or touching individual elements (smartphone) additional information about a given device will be displayed.




# 7. JSON data format

## 7.2 Decrypted JSON data

The statistics JSON - array ***data*** contains information about the **iNode LoRa GSM MQTT**:

- timestamp – time stamp in seconds (Unix timestamp)
- type – name
- mac – mac address
- ip – IP address in the GPRS network
- rtc – device time in seconds (Unix timestamp)
- scnt – number of GPRS sessions since power on or reset
- frm – firmware version
- rRx – number of radio frames received by iNode LoRa GSM MQTT
- rTx – number of radio frames sent by iNode LoRa GSM MQTT
- workTime – device operation time in seconds from power on or reset
- txp – set LoRa output power in dBm
- rst – number of device resets
- temp – the device temperature in °C
- msg – number of JSON data transmissions
- ack – number of confirmed JSON data transmissions
- tx_time – JSON data sending time in microseconds
- vbat – modem supply voltage in mV
- period – the period of sending JSON data
- manuf – device type code
- rstr – reason for last reset
- imsi – the unique number of the SIM card

- imei – the unique modem number
- rssi – GSM signal level in dBm
- lac – specifies BTS
- ci – specifies BTS
- oper – GSM operator

**topic iNode/LoRa-GSM/D1F0256E7095 (statistical data about iNode LoRa GSM)**

{"data": [{"timestamp": "2020-05-17T19:08:20Z","type": "iNode-LoRa-GSM:D1F0256E7095","mac": "D1F0256E7095","ip": "100.70.25.63","rtc": 1589742500,"scnt": 1,"frm": "May 17 2020/20:44:42","rRx": 38,"rTx": 28,"workTime": 682,"txp": 14,"rst": "","temp": 25,"msg": 40,"ack": 39,"tx_time": 1576000,"vbat": 3903,"period": 60,"manuf": 188,"rstr": 1536,"imsi": "260021872763623","imei": "862927041535668","rssi": -85,"lac": "E330","ci": "BFD8","oper": "26002"}]}

The JSON data - the array ***data*** contains information about the sensor:

- timestamp – time stamp in seconds (Unix timestamp)
- mac – mac address
- rssi – LoRa signal level from the sensor in dBm
- snr – LoRa noise signal ratio from the sensor in dBm (only LoRa mode)
- rawData – basic frame from the sensor
- rawResp – frame with the answer to the active query (only GFSK mode)

**topic iNode/LoRa-GSM/D1F0256E7095/D1F02565D5CE**

{"data": [{"timestamp": "2020-05-17T19:08:50Z","mac": "D1F02565D5CE","rssi": -89,"snr": 1,"rawData": "26FF038FB0AE81424D001C000A00150025000A00150025076802540 09D0038001A000497000382020A14","rawResp": ""}]}

**topic iNode/LoRa-GSM/D1F0256E7095/D1F0258AC2A6**

{"data": [{"timestamp": "2020-05-17T19:08:54Z","mac": "D1F0258AC2A6","rssi": -26,"snr": 24,"rawData": "0EFF90820000B73E0000E803C00060020A04","rawResp": ""}]}

**topic iNode/LoRa-GSM/D1F0256E7095/D1F0257254B4**

{"data": [{"timestamp": "2020-05-17T19:08:56Z","mac": "D1F0257254B4","rssi": -70,"snr": 25,"rawData": "19FF909B0090000000002D184D237A5A172C9501B3AA1A4052E6020A0E","rawResp": ""}]}

## 7.3 JSON encrypted data:

In case the data from **iNode LoRa GSM MQTT** is encoded at the beginning of the JSON file is the ***key*** field. This is the temporary key used to encrypt JSON data. It is encrypted with a master key entered into **iNode LoRa GSM MQTT**. The data is encrypted with the ARCFour algorithm.

{"key": "33FE46D546832247CC91A8EA733D56E9","data": [Q}H/kk_ {.m Z u Ö - G z| Tw e Zn&v1 H T} qE l m qq O J)};)x m n +e UC lA7! j * @ ]+ /k'v 0Ee 3@^f[+ ">
y aK B\ 9: l B]k A6 hY(} w |SL_h)
j .xOLT S @
T h_O
Q1 ]}

## 7.4 Decrypting JSON data

The following function example functions in JavaScript decoding JSON encrypted data. The jsaes.js file can be downloaded from:
https://support.inode.pl/apps/iNodeMqttMonitor/js/jsaes.js

```
/*
 * RC4 symmetric cipher encryption/decryption
 * @license Public Domain
 * @param string key - secret key for encryption/decryption
 * @param string str - string to be encrypted/decrypted
 * @return string
 */

var rc4_s = [];
var rc4_i;
var rc4_j;

function rc4_init(rc4_key, rc4_key_length)
{
   var j = 0, x;
   for (var i = 0; i < 256; i++) {
      rc4_s[i] = i;
   }
   for (i = 0; i < 256; i++) {
      j = (j + rc4_s[i] + rc4_key[i % rc4_key_length]) % 256;
      x = rc4_s[i];
      rc4_s[i] = rc4_s[j];
      rc4_s[j] = x;
   }

   rc4_i=0;
   rc4_j=0;
}

function rc4_get_xor_byte()
{
   var x;

   rc4_i = (rc4_i + 1) % 256;
   rc4_j = (rc4_j + rc4_s[rc4_i]) % 256;
   x = rc4_s[rc4_i];
   rc4_s[rc4_i] = rc4_s[rc4_j];
   rc4_s[rc4_j] = x;
   return rc4_s[(rc4_s[rc4_i] + rc4_s[rc4_j]) % 256];
}

var JSON_USER_KEY = new Array(16);
var JSON_DECRYPT_KEY = new Array(16);

function searchCommentValue(sstr, key)
{
   var offset_start=sstr.search(key);

   if(offset_start>=0)
   {
      var rsstr=sstr.slice(offset_start+key.length);
      var offset_end=rsstr.search('"');
```

```
      return rsstr.substring(0,offset_end);
   }
   else
   {
      return "";
   }
}

function decodeJSON(json_raw, json_key)
{
   var img_dataView = new DataView(json_raw);
   var ik;
   var img_byte;
   var xor_byte=0;
   var ik_img_offset=0;

   for(var i = 0; i < 16; i++)
   {
      JSON_USER_KEY[i] = 0;
   }

   for(var i = 0; i < json_key.length; i+=2)
   {
      JSON_USER_KEY[15-i] = json_key.charCodeAt(i+1);
      JSON_USER_KEY[14-i] = json_key.charCodeAt(i);
   }

   var JSON_KEY=searchCommentValue(ab2str(json_raw),'{"key": "');

   if(JSON_KEY.length!=0)
   {
      AES_Init();
      var block = new Array(16);
      for(var i = 0; i < 16; i++)
        { block[15-i] = parseInt(JSON_KEY.substr(i*2,2), 16) };

      var key = new Array(16);
      for(var i = 0; i < 16; i++)
         { key[i] = JSON_USER_KEY[i]; }

      AES_ExpandKey(key);
      AES_Decrypt(block, key);

      for(var i = 0; i < 16; i++)
         { JSON_DECRYPT_KEY[15-i] = block[i] };

      AES_Done();
      rc4_init(JSON_DECRYPT_KEY,16);

      var json_data_start=ab2str(json_raw).search(',"data": ')+10;

       for(ik=json_data_start;ik<(img_dataView.byteLength-2);ik++)
      {
         img_byte=img_dataView.getUint8(ik);

         img_dataView.setUint8(ik,(img_byte^rc4_get_xor_byte())& 0xff);
      }
   }
   return json_raw;
}
```

# 8. TECHNICAL SPECIFICATIONS

GFSK/LoRa radio parameters:

- RX/TX:
  - ISM: 868 MHz;
- output power (minimum / maximum):
  - ISM: 2dBm / 20dBm;
- modulation:
  - GFSK;
  - LoRa - CSS (chirp spread spectrum) modulation;
- external antenna:
  - SMA antenna connector- female;
  - frequency: 868 MHz;
  - average gain: 3dBi;

GFSK/LoRa:

- configurable from PC:
  - GFSK modulation: frequency, power, bandwidth, bit rate, deviation;
  - LoRa modulation: frequency, power, bandwidth, sf, cr;
  - TX power in range from +2dBm to +20dBm;
  - device access password;
  - GPRS network parameters – APN name, user and password;
  - device name in the GSM/GPRS network;
  - password for verifying messages received from sensors;
  - MQTT server parameters;
  - JSON data filter;

GSM/GPRS :

- Fibocom G510 GPRS meeting the essential requirements of Article 3 of the R&TTE Directive 1999/5/EEC, which is used in accordance with the manufacturer's intended use and recommendations and has the CE0700 marking:
  - Quad Band 900/1800MHz 850/1900MHz;
  - Multi-slot class 10 (4 Down; 2 Up; 5 Total) Max BR Downlink 85.6 Kbps Coding Scheme CS1-CS4;

GSM antenna connector:

- SMA type – female;
- recommended antenna parameters:
  - frequency: Quad Band: 850/900/1800/1900 MHz
  - gain: 0 dBi, but no more than 2,5dBi
  - impedance: 50 Ω
  - VSWR: 1,5:1; in the worst case 2,5:1

Power supply:

- micro USB socket for connecting external power supply stabilized 230V 50Hz AC / DC 5V 1000mA with double or reinforced insulation;
- maximum connection cable length: 3 m;

Housing:

- metal;
- dimensions: 60 mm x 38 mm x 22 mm (LxWxH);

Others:

- firmware upload and configuration option via USB – WebUSB feature;
- nano SIM connector;
- dual color LED: red / green;
- operating temperature: from -30 to 65°C;

- humidity: 35-90% RHG;
- weight: 50 g ;

Equipment:

- external antenna. ISM 866 MHz, 2dBi gain, with SMA male plug connector;
- external antenna, GSM, dual band, 900/1800 MHz, 2dBi gain, with SMA male plug connector;

Software:

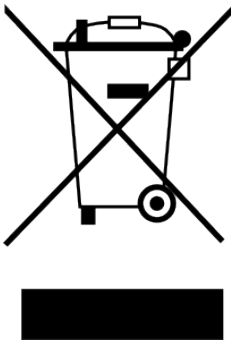
- Google CHROME: Android OS, Linux, Windows 10;

Chipset:

- STM32L082;
- SX1276;

*The manufacturer reserves the right to change device and software parameters as well as introduce other construction solutions.*

# 9. CORRECT PRODUCT REMOVAL (WASTE ELECTRICAL AND ELECTRONIC EQUIPMENT)



The packaging materials are 100% suitable for use as a secondary raw material. The packaging should be disposed of in accordance with local regulations. Keep packaging materials out of the reach of children as they pose a source of danger. The marking on the product or in related texts indicates that the product should not be disposed of with other household waste after it has expired. To avoid harmful effects on the environment and human health due to uncontrolled waste disposal, please separate the product from other types of waste and recycle responsibly to promote the reuse of material resources as a permanent practice.

Correct disposal of the device:

- Pursuant to the WEEE Directive 2012/19 / EU, the symbol of the crossed wheeled waste container means all electrical and electronic devices subject to selective collection.
- After the end of its useful life, this product must not be disposed of as normal household waste, but should be sent to a collection point for the recycling of electrical and electronic equipment. This is indicated by the symbol of the crossed-out wheeled waste container, placed on the product or in the operating instructions or packaging.
- The materials used in the device are reusable according to their designation. Thanks to the reuse, use of materials or other forms of use of used devices, you make a significant contribution to the protection of our natural environment.
- For information on the appropriate disposal point for used electrical and electronic equipment, please contact your local municipality administration or the device seller.
- Used, fully discharged batteries and accumulators must be disposed of in specially marked containers, taken to special waste collection points or sellers of electrical equipment.
- Users in companies should contact their supplier and check the terms of the purchase contract. The product should not be disposed of with other household waste.

Numer Deklaracji 2/02/2018 Data wystawienia Deklaracji 03.02.2018 r.
*Number of declaration of Conformity* *Date of issue of declaration*

## DEKLARACJA ZGODNOŚCI UE RED
*UE RED DECLARATION OF CONFORMITY*

Producent / *Manufacturer*:

**ELSAT s.c.**

*(nazwa producenta / producer's name)*

ul.Warszawska 32E/1, 05-500 Piaseczno k/Warszawy

*(adres producenta / producent's address)*

*niniejszym deklaruje, że następujący wyrób:*
*declare, under our responsibility, that the electrical product:*

**iNode LoRa GSM MQTT** **0xB704, 0xB708**

*(nazwa wyrobu / product's name)* *(model / model)*

spełnia wymagania następujących norm zharmonizowanych:
*to which this declaration relates is in conformity with the following harmonized norm:*

Assessment of the compliance of low power electronic and electrical equipment with the basic restrictions related to human exposure to electromagnetic fields (10 MHz to 300 GHz):

**PN-EN 62479:2011**

Short Range Devices (SRD) operating in the frequency range 25 MHz to 1 000 MHz**:**

**ETSI EN 300 220-1 V 3.1.1:2017-02**

**ETSI EN 300 220-2 V 3.1.1:2017-02**

Radio Spectrum ISM (Article 3.2 of the RED directive)**:**

**ETSI EN 300 328 V2.1.1:2016-11**

EMC (Article 3.1.b of the RED directive):

**ETSI EN 301 489-1 V2.1.1:2016-11**

**ETSI EN 301 489-3 V2.1.1:2016-11**

**ETSI EN 301 489-17 V3.1.1:2016-11**

Safety (Article 3.1.a of the RED directive):

**PN-EN 62368-1:2015-03**

Health (Article 3.1.a of the RED directive):

**PN-EN 62311:2008**

RoHs:

**PN-EN IEC 63000:2019-01**

*jest zgodny z postanowieniami następujących dyrektyw Unii Europejskiej:*
*is compatible with the following European Union directives:*

**Dyrektywa RED 2014/53/UE**
**Dyrektywa EMC 2014/30/UE**
**Dyrektywa LVD 2014/35/UE**
**Dyrektywa RoHS 2011/65/UE**

*Procedura oceny zgodności: wewnętrzna kontrola produkcji zgodnie z załącznikiem II RED*
*Acceptance procedure: internal production control in accordance with Annex II of the RED Directive*

03.02.2018 r. Robert Kujda
Piaseczno k/Warszawy

*(data i miejscowość / date and place)*

Współwłaściciel

*(podpis i stanowisko / signature and function)*

RoHS 2 2011/65/EU