iNode LAN Central

instrukcja użytkownika

1. Wstęp

Chcielibyśmy Państwu przedstawić rodzinę urządzeń **iNode** działających w technologii **Bluetooth Low Energy ®**. Pokażemy Państwu, że BLE to nie tylko tagi do znajdowania zagubionych kluczy, czy tagi lokalizacyjne, lecz jeszcze coś więcej.

Nasze urządzenia potrafią to i jeszcze więcej:

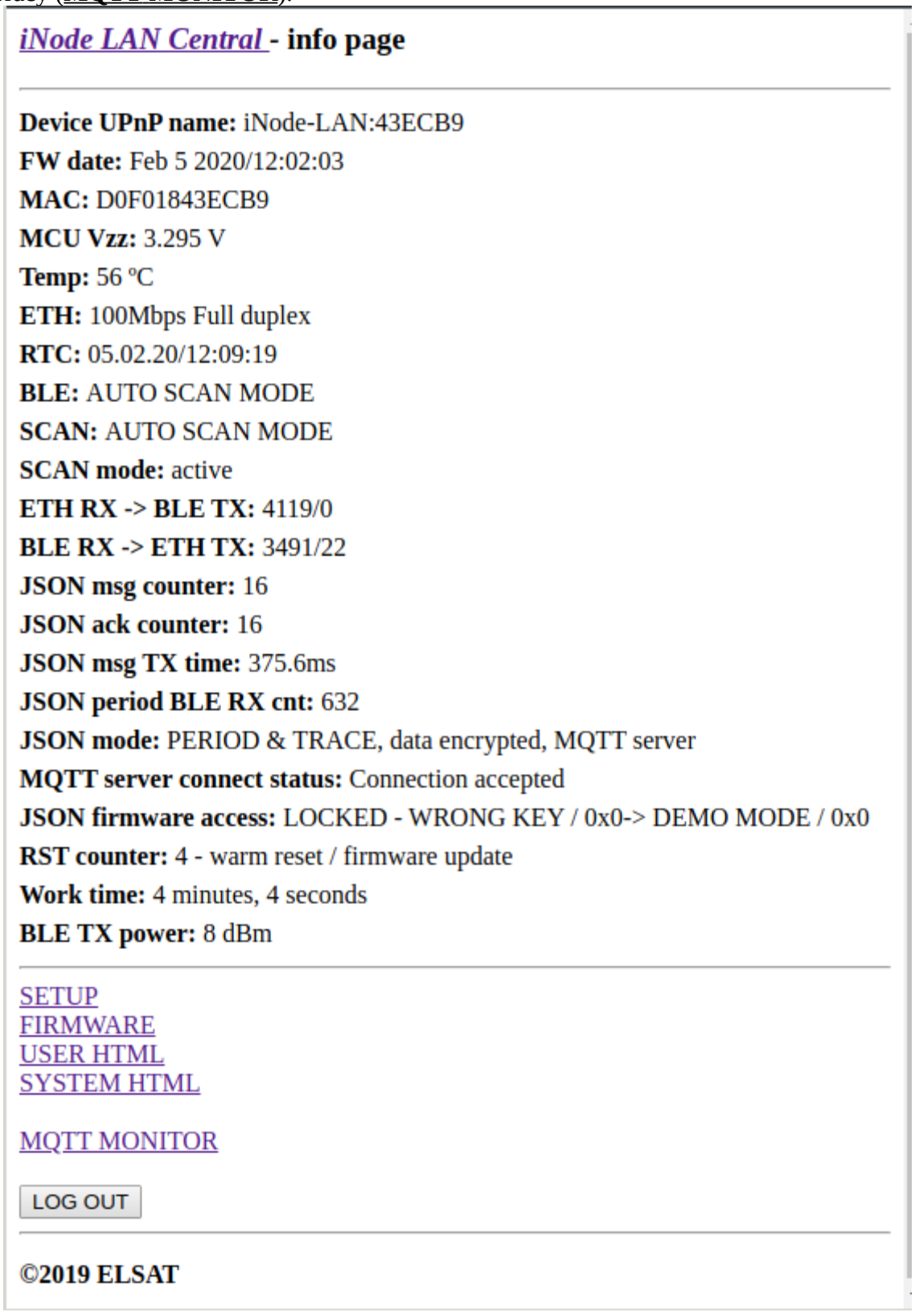
- Są to przede wszystkim urządzenia bateryjne.
- Działają bez jej wymiany do 12 miesięcy w zależności od zastosowania i sposobu użycia.
- Mają pamięć do rejestrowania zdarzeń, odczytów pomiarów etc.
- Precyzyjne czujniki temperatury, wilgotności, przyspieszenia czy pola magnetycznego pozwalają na precyzyjne sterowanie automatyką domową czy też opiekę nad ludźmi starszymi.
- Jako urządzenia zdalnego sterowania, mimo małego poboru mocy, mają duży zasięg i cechy niedostępne dla innych konkurencyjnych urządzeń – własne hasło użytkownika, szyfrowanie AES, sterowanie bezpośrednio ze smartfona.

iNode może też pomóc w kontroli przemieszczania się osób czy towarów, zapisując czas pojawienia się i zniknięcia z zasięgu rejestratora (aktywne **RFID®** o dużym zasięgu). Nowe funkcjonalności związane z rozwojem produktu to też nie problem – umożliwia to zdalna wymiana firmware z PC lub smartfona z **Bluetooth 4.0 ®** i obsługą **Bluetooth Low Energy ® (Bluetooth Smart ®)**.

iNode LAN Central umożliwia zaistnienie urządzeń z BLE (*Bluetooth Smart*, IoT - *Internet of Things*) w sieciach z protokołem ethernet: LAN, Wi-Fi czy Internet. Zapewnia on wysyłanie w formacie JSON na serwer MQTT lub HTTP/POST danych odbieranych z czujników **iNode Care** lub innych urządzeń BLE. Dane mogą być szyfrowane dzięki czemu użytkownik może korzystać z publicznego serwera MQTT lub HTTP. Odkodowywanie danych odbywa się dopiero w aplikacji np. iNode MQTT Monitor.

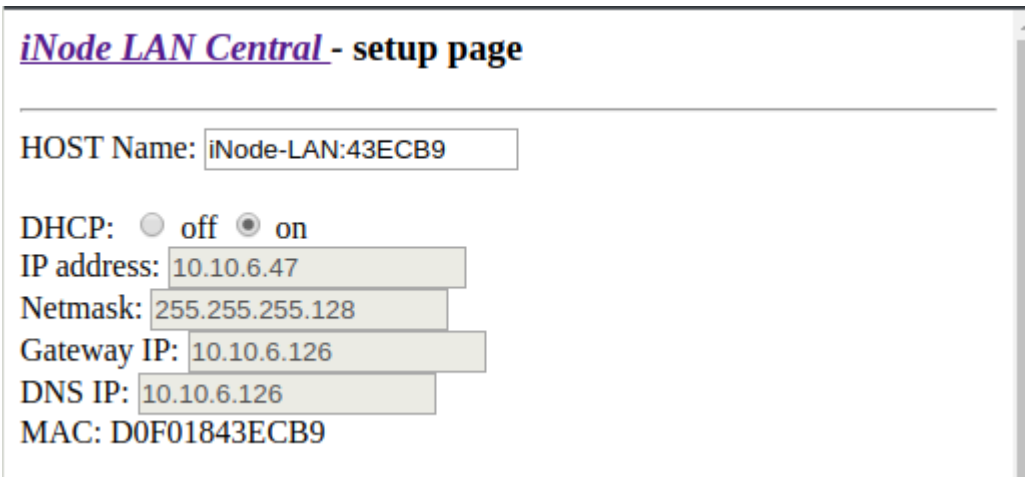
2. Konfiguracja iNode LAN Central

Urządzenie domyślnie ma włączone DHCP – w ten sposób uzyskuje adres w sieci LAN 10/100Mbps. Po wpisanie tego adresu IP w przeglądarce powinna wyświetlić się następująca strona, która wyświetla informacje statystyczne na temat urządzenia, jego nazwę, temperaturę, czas pracy od ostatniego resetu, itp. Można z niej wybrać dalsze strony służące do konfiguracji pracy urządzenia (**SETUP**, **FIRMWARE**, **USER HTML, SYSTEM HTML**) lub przetestowania jego pracy (**MQTT MONITOR**).



2.1. SETUP

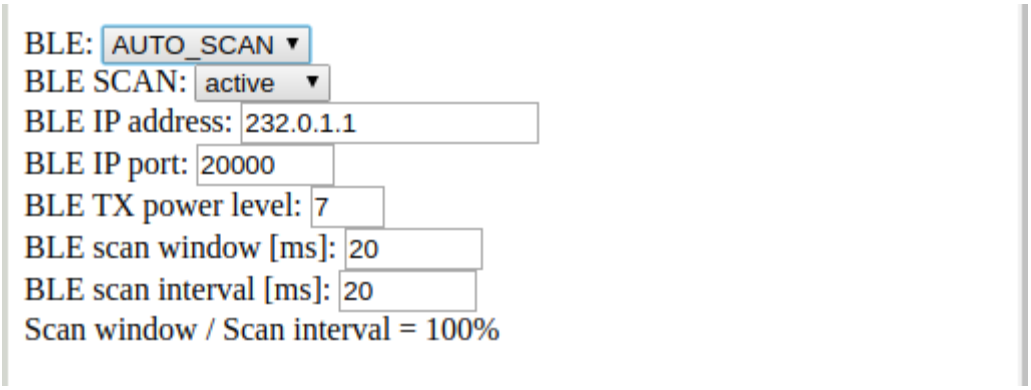
Strona **SETUP** umożliwia zmianę sposobu uzyskiwania adresu IP przez urządzenie.



Jeżeli jest zaznaczone ***DHCP off*** to pola ***IP address***, ***Netmask***, ***Gateway IP***, ***DNS IP*** są aktywne i należy do nich wpisać takie adresy i wartości, żeby **iNode LAN Central** mógł pracować w sieci ethernet. Domyślnie DHCP jest włączone co oznacza, że wszystkie te parametry sieciowe zostaną pobrane z serwera DHCP, który jest przeważnie udostępniany np. przez router ADSL.

Użytkownik może zmienić domyślną nazwę urządzenia w polu ***HOST name*** na dowolną inną. Może ona mieć maksymalnie 16 znaków długości. Niewskazane jest np. używanie polskich znaków diakrytycznych z tego względu, że mogą być niewłaściwie interpretowane przez inne urządzenia sieciowe.

Jeśli chodzi o BLE to **iNode LAN** Central może pracować w dwóch trybach:



1. **AUTO SCAN** - po włączeniu zaczyna skanować BLE w swoim otoczeniu (w trybie aktywnym) i wysyła rezultaty do sieci LAN pakietami IP/UDP jako multicast/unicast lub broadcast. W przypadku włączonego multicast odbiera dane z innych urządzeń w sieci LAN np. **iNode LAN**. Tak więc jeden **iNode LAN Central** może wysyłać na seerwer MQTT lub HTTP/POST dane obierane przez BLE lub docierające do niego przez LAN.

   Multicast – to taki sposób wysyłania pakietów IP, że trafiają do wielu urządzeń, ale tylko takich, które ich używają – określa się to przez podanie grupy multicastowej i portu. Dla iNode-LAN jest to 232.0.1.1:20000. Unicast to jeden unikalny adres IP w sieci Internet lub w sieci lokalnej. Broadcast to taki sposób wysyłania pakietów IP, że trafiają do wszystkich

urządzeń w sieci lokalnej. Prosty, ale jednocześnie wytwarzający niepotrzebny ruch pakietów IP w niektórych miejscach sieci.

2. **OFF** - po włączeniu zasilania urządzenie nie jest w żaden sposób aktywne w BLE. Z programu typu telnet np. Hyperterminal.exe można się połączyć z **iNode LAN** Central na porcie 5500. Działa ono wtedy tak samo jak **iNode Serial Transceiver USB** przez COM, to znaczy obsługuje ten sam protokół.

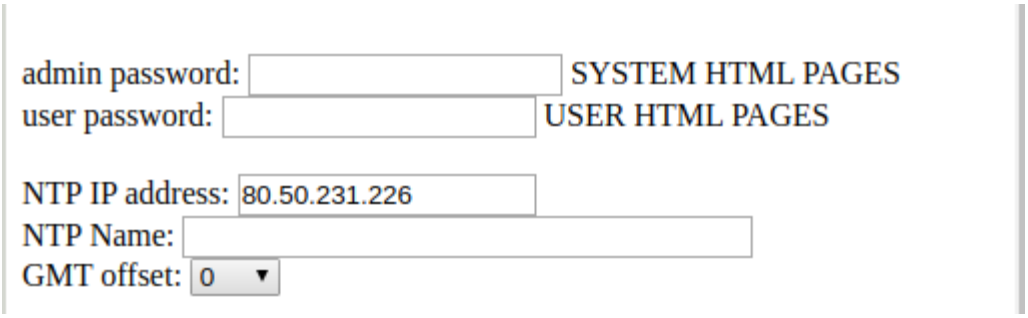
W **BLE SCAN** można wybrać rodzaj skanowania: ***passive*** (pasywne – czyli bez uzyskiwania dodatkowych informacji z urządzeń BLE) i ***active*** (aktywne – każde wyskanowane urządzenie BLE jest dodatkowo odpytywane co wpływa na trwałość jego baterii).

Pola ***BLE IP address*** i ***BLE IP port*** służą do podania adresu IP i portu serwera do którego będą wysyłane pakiety UDP z danymi z pakietów BLE odebranych podczas skanowania BLE (dla trybu **AUTO SCAN**).

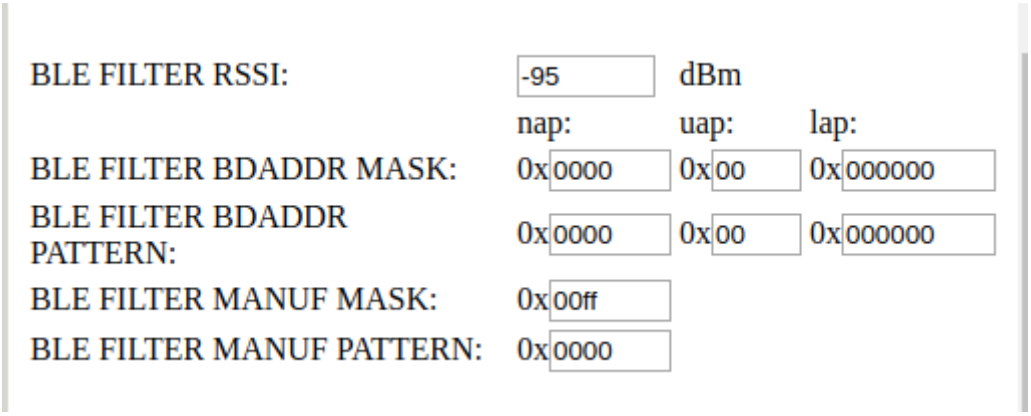
Pole ***BLE TX power level*** służy do podania z jaką mocą odbywa się nadawanie pakietów BLE podczas aktywnego skanowania. Zależność pomiędzy poziom mocy a wartością mocy wyrażoną w dBm podaje poniższa tabelka:

BLE TX power level	***TX Power [dBm]***
0	-18
1	-12
2	-10
3	-4
4	-2
5	+2
6	+6
7	+8

Wartości w polach ***BLE scan window*** i ***BLE scan interval*** określają przez ile czasu urządzenie skanuje (***BLE scan window)***.



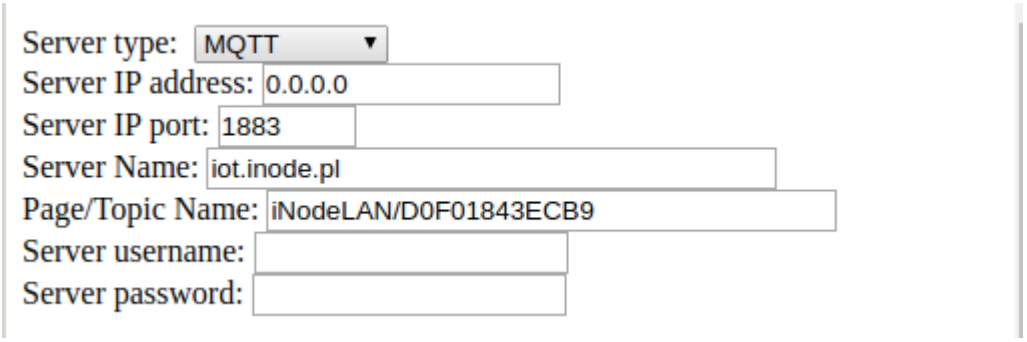
W polach ***admin password*** i ***user password*** można podać hasło do stron systemowych urządzenia (***admin password***) lub stron wgranych przez użytkownika (***user password***).



Powyższe parametry umożliwiają filtrowanie urządzeń BLE do wysyłania informacji o nich w formacie JSON.
BLE FILTER RSSI – poziom progowy sygnału; przez dalsze filtry uwzględniane są tylko urządzenia z których odbierany poziom sygnału jest większy od tego tu ustawionego.
BLE FILTER BDADDR MASK – maska adresu BDADDR.
BLE FILTER BDADDR PATTERN – wzorzec adresu BDADDR z którym jest porównywany odebrany BDADDR po operacji AND z maską BDADDR.
BLE FILTER MANUF MASK – maska dla Manufacturer Specific Data.
BLE FILTER MANUF PATTERN – wzorzec dla Manufacturer Specific Data.

Pole ***NTP IP address*** służy do podania adresu IP serwera NTP. Jeżeli serwer nie zostanie odnaleziony ze względu na błędny adres to czas w urządzeniu nie będzie prawidłowy lecz urządzenie będzie działać. ***GMT Offset*** określa przesunięcie godzinowe w stosunku do czasu GMT (strefę czasową) w zakresie od -12 do 12 godzin.

Dalej możemy ustawić parametry serwera MQTT lub HTTP/POST z którym urządzenie ma współpracować:

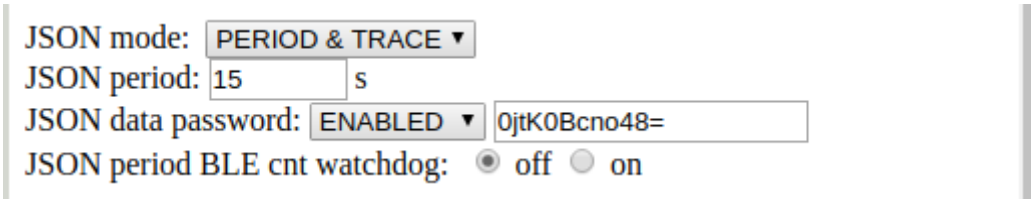


Przed wszystkim należy wybrać typ serwera – ***Server type,*** podać jego adres IP – ***Server IP address*** lun nazwę – ***Server Name***. Domyślne ustawienia urządzenia umożliwiają współpracę z serwerem MQTT iNode – iot.inode.pl

W przypadku serwera HTTP należy podać jego nazwę - ***Server Name***, port (dla HTTP powinien to być domyślnie port 80) – ***Server IP port*** oraz nazwę skryptu wywoływanego przez urządzenie przy wysyłaniu danych przez POST – ***Page/Topic Name***.

Dodatkowo można podać nazwę użytkownika – ***Server username*** i hasło – ***Server password*** jeżeli dostęp do serwera MQTT lub HTTP/POST tego wymaga.

Kolejne ustawienia dotyczą formatu danych JSON:



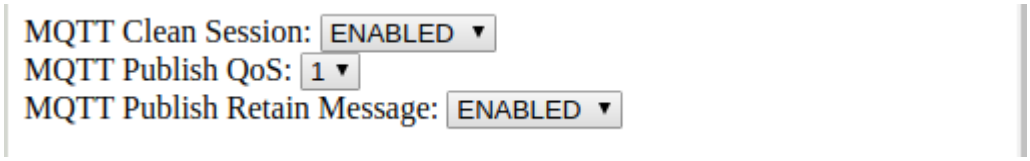
Są trzy możliwe tryby zbierania danych JSON – ***JSON mode***:

1. **STOP –** urządzenie nie wysyła danych w formacie JSON.
2. **PERIOD & TRACE** – urządzenie zbiera dane o urządzeniach BLE w swoim otoczeniu i docierających do niego przez LAN. Żeby urządzenie zostało usunięte z listy musi być poza zasięgiem (nie przesyłać pakietów BLE przez ok. 30 sekund). Na liście może być ok. 24 urządzeń jednocześnie.
3. **PERIOD & CLEAR** - urządzenie zbiera dane o urządzeniach BLE w swoim otoczeniu i docierających do niego przez LAN. Po każdej wysyłce danych w formacie JSON na serwer lista jest kasowana. Na liście może być ok. 24 urządzeń jednocześnie.

Okres wysyłania danych jest ustalany przez wpisanie odpowiedniej wartości wyrażonej w sekundach w polu ***JSON period***. Minimalna wartość to 2 sekundy i jest zależna od szybkości wysyłania danych na serwer MQTT lub HTTP/POST.

iNode LAN Central może szyfrować wysyłane dane w formacie JSON – ***JSON data password***. W tym celu należy włączyć szyfrowanie – **ENABLED** oraz wpisać hasło – maksymalnie 16 znaków. To samo hasło trzeba później wpisać do aplikacji **iNode MQTT Monitor**, aby mogła odkodować dane. Przy operacji przywracania domyślnych ustawień urządzenia – włączenie zasilania z wciśniętym przyciskiem od spodu urządzenia – tworzone jest nowe losowe hasło.

Funkcja ***JSON period BLE cnt watchdog***, jeśli jest włączona, resetuje urządzenie, gdy w czasie ***JSON period*** nie zostaną odebrane z BLE lub LAN żadne dane. Dodatkowo w urządzenie wbudowana jest funkcjonalność resetu urządzenia po połowie czasu dzierżawy pobranego z DHCP.



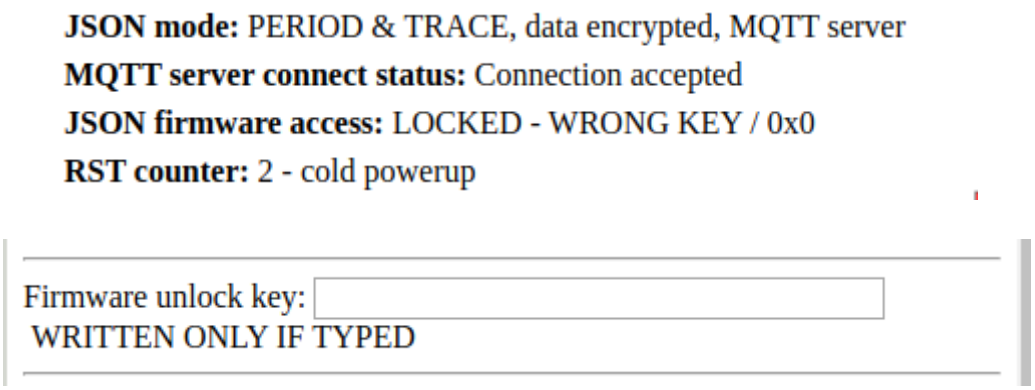
Powyższe ustawienia dotyczą tylko serwera MQTT. Jeśli ***MQTT Publish Retain Message*** – jest włączone – ***ENABLED***, to ostatni wysłany komunikat jest zapamiętywany przez serwer MQTT. Znaczenie ***MQTT Publish QoS*** jest następujące:

- ***QoS 0*** - klient nie otrzyma od serwera żadnego potwierdzenia. Podobnie wiadomość dostarczona klientowi z serwera nie musi być potwierdzona. Jest to najszybszy sposób publikowania i odbierania wiadomości, ale także ten, w którym najprawdopodobniej nastąpi utrata wiadomości.
- ***QoS 1*** - klient otrzyma wiadomość potwierdzającą z serwera po jej opublikowaniu. Jeśli oczekiwane potwierdzenie nie zostanie odebrane w określonym czasie, klient musi ponowić wiadomość. Wiadomość otrzymana przez klienta również musi zostać potwierdzona na czas, w przeciwnym razie serwer ponownie dostarczy wiadomość.

Firmware dla **iNode LAN Central** może być wgrany do **iNode LA**N. Jednak w przypadku, gdy w **iNode LAN** nie ma wpisanego prawidłowego klucza odblokowującego firmware – ***Firmware***

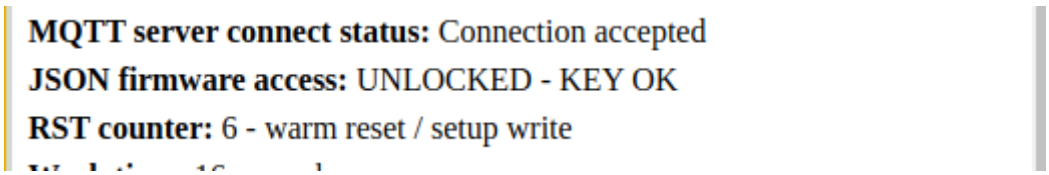
unlock key, po 15 minutach od włączenia, w wysyłanych w formacie JSON danych nie będzie informacji o urządzeniach BLE:

JSON firmware access*: LOCKED - WRONG KEY / 0x0* – JSON nie zawiera danych BLE; iNode MQTT Monitor nie pokazuje żadnych urządzeń BLE lub pokazuje przy nich czerwone przekreślone kółko.
JSON firmware access*: LOCKED - WRONG KEY / 0x0-> DEMO MODE / 0x0.* - JSON zawiera dane BLE; 15 minut po włączeniu urzadzenia.



Przykład wpisywania kodu

oraz status urządzenia jeżeli wpisany kod jest prawidłowy:



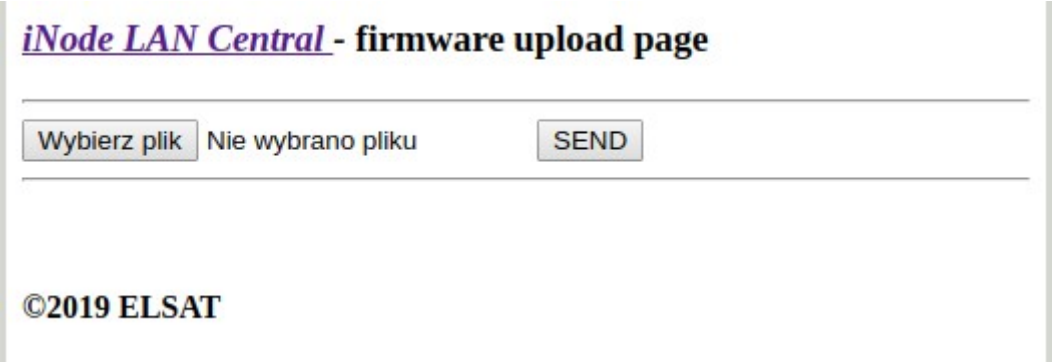
Każde **iNode LAN Central** ma firmware odblokowany fabrycznie. Nie można wtedy podać nowego klucza. Klucz nie jest zostanie skasowany nawet przy wymianie firmware na firmware dla **iNode LAN**.

Żeby zmienione ustawienia zostały zapisane w urządzeniu należy wcisnąć przycisk ***SAVE***. Poprawne wpisanie zostanie potwierdzone komunikatem ***done: OK***. Po około 3-5 sekundach nastąpi reset urządzenia, aby nowe ustawienia zostały uwzględnione. Przy zmianie parametrów sieci ethernet należy uważać, żeby nie podać adresów spoza sieci LAN.

Ustawienia domyślne można przywrócić włączając zasilanie urządzenia przy naciśniętym przycisku RESET znajdującym się w otworze od spodu urządzenia.

2.2. FIRMWARE

Strona **FIRMWARE** umożliwia wpisanie nowego firmware do urządzenia.

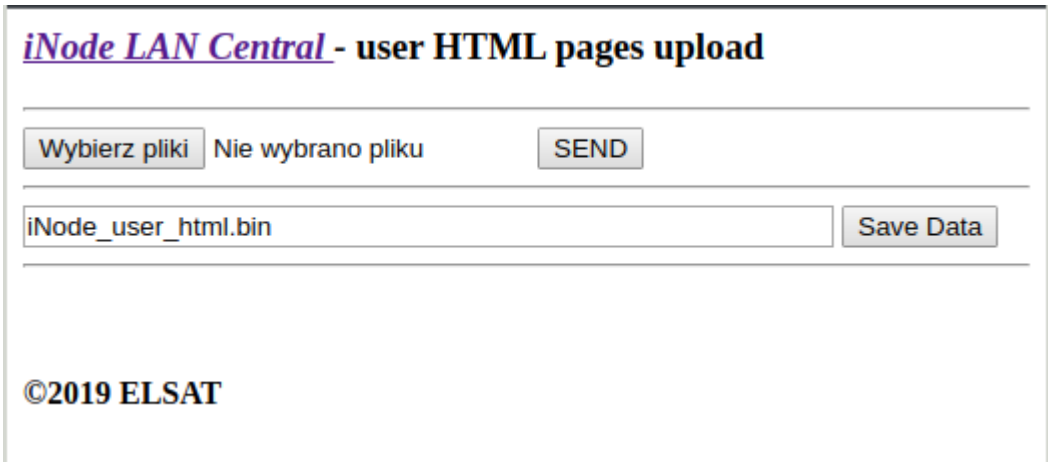


Po wybraniu przycisku ***Przeglądaj*** możemy wybrać plik z nowym firmware dla danego urządzenia. Wysłanie firmware następuje po naciśnięciu przycisku ***SEND***. Pojawia się wtedy komunikat ***uploading ...***, który jeżeli przesłanie pliku uda się zostanie zastąpiony przez ***done: OK***. Następnie pojawi się komunikat ***restarting ...***, który jeżeli wymiana firmware zakończy się powodzeniem zostanie zastąpiony przez ***done: OK***. Następnie po 3-5 sekundach urządzenie zostanie zrestartowane. W przypadku włączonego DHCP należy odczekać chwilę, aż urządzenie pobierze na nowo parametry sieciowe z serwera DHCP – dioda LED przy złączu RJ45 miga wtedy szybko. Wolne miganie diody LED oznacza pobranie parametrów sieciowych przez DHCP.

Pliki ***fep***, instrukcje lub oprogramowanie użytkowe jest do pobrania w serwisie pomocy technicznej: http://support.inode.pl/.

2.3. USER HTML

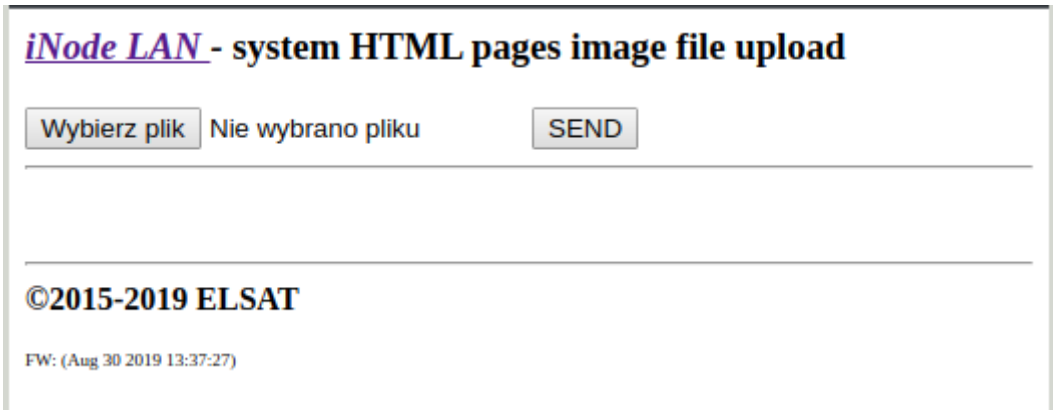
Strona **USER HTML** umożliwia wpisanie do urządzenia stron własnych użytkownika. Na strony te jest przeznaczone 2,9MB pamięci. Wszystkie pliki powiązane ze stronami (obrazki, skrypty itp.) powinny być umieszczone w jednym katalogu. Może ich być maksymalnie 512, a ich nazwy mogą mieć maksymalnie 40 znaków.



Po wybraniu przycisku ***Przeglądaj*** możemy wybrać pliki stron html i powiązanych z nimi obrazków lub skryptów. Wysłanie ich do urządzenia następuje po naciśnięciu przycisku ***SEND***. Pojawia się wtedy komunikat ***reading files: done, uploading file of xxx kbytes***, który jeżeli przesłanie pliku uda się zostanie zastąpiony przez ***done: OK***. Wysłany do urządzenia obraz pamięci ze stronami HTML można zapisać na lokalnym dysku po naciśnięciu przycisku ***Save Data***.

2.4. SYSTEM HTML

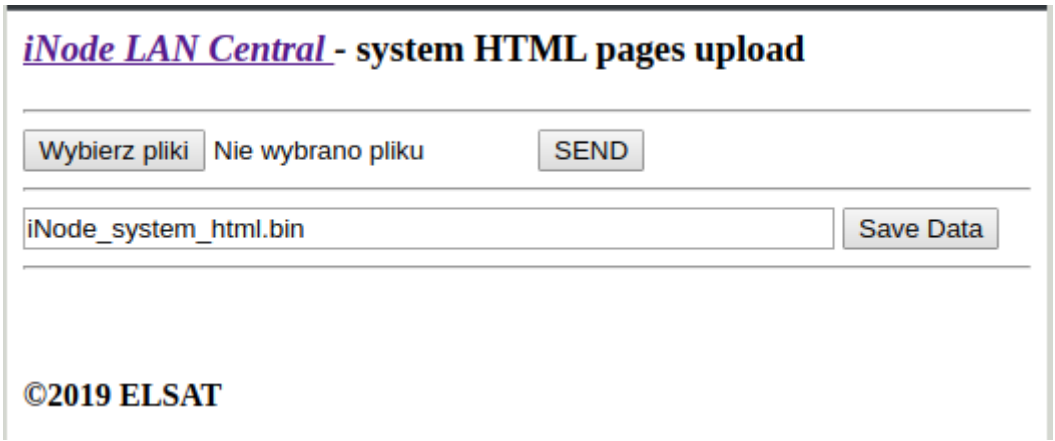
Strona **SYSTEM HTML** umożliwia wymianę stron systemowych. Plik ze stronami w identycznym formacie jak te użytkownika wgrywa się do obszaru stron systemowych z użyciem strony *flash.cgi* (jest ona zawsze dostępna bezpośrednio). Może to być również jeden plik ze stronami w formacie bin.



Po wybraniu przycisku ***Przeglądaj*** możemy wybrać obraz stron systemowych. Wysłanie go do urządzenia następuje po naciśnięciu przycisku ***SEND***. Pojawia się wtedy komunikat ***uploading ...***, który jeżeli przesłanie pliku uda się zostanie zastąpiony przez ***done: OK***. Na dole strony podana jest data firmware w urządzeniu: FW: (.....).

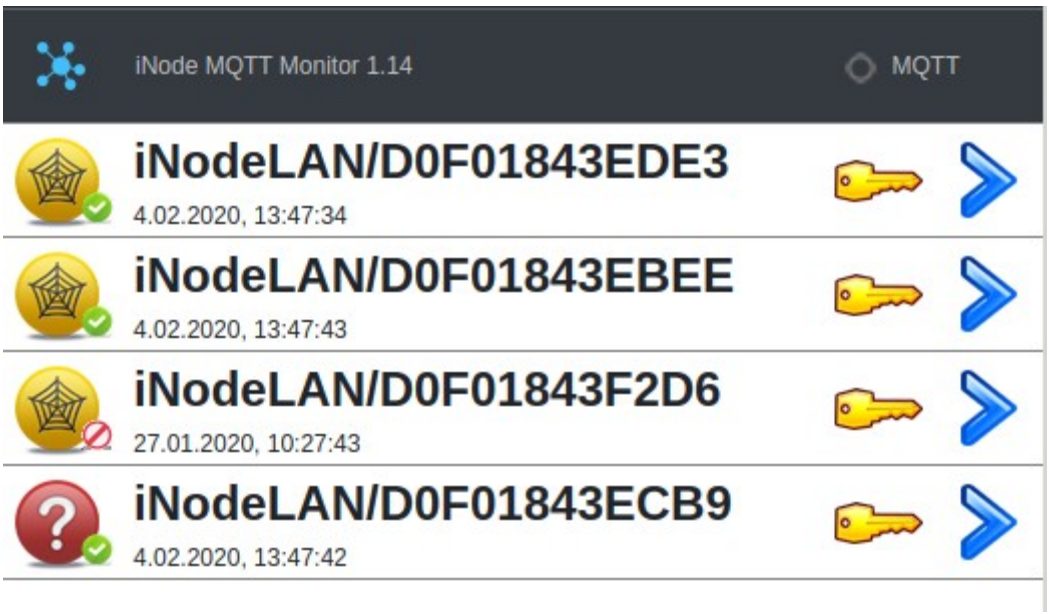
W przypadku braku stron systemowych HTML w urządzeniu przeglądarka może wyświetlać prośbę o hasło lub inne błędy. Dzieje się tak przeważnie przy wgraniu pliku bin ze stronami HTML użytkownika jako systemowych. Należy wtedy ponownie wpisać do urządzenia systemowe strony HTML używając do tego strony flash.cgi.

Użytkownik może utworzyć własny obraz stron systemowych wykorzystując stronę *system_flash_html.shtml* Robi się to w sposób identyczny jak w przypadku stron HTML użytkownika.



2.5. MQTT MONITOR

Strona **MQTT MONITOR** - https://support.inode.pl/apps/iNodeMqttMonitor/ umożliwia przetestowanie komunikacji pomiędzy urządzeniem, a serwerem MQTT lub HTTP/POST. Obsługuje również adaptery USB BT lub LPWAN oraz wspomaga technologię Web Bluetooth. Umożliwia zdalne sterowanie urządzeniami np. wyjściem w **iNode MCU Relay**. Aplikacja **iNode MQTT Monitor** jest dedykowana dla przeglądarki Google Chrome i działa na systemach operacyjnych Android, Windows, Linux itp. Po wczytaniu się aplikacji można ją zainstalować w celu późniejszego łatwiejszego uruchamiania. Na głównym ekranie pojawi się wtedy ikona aplikacji.

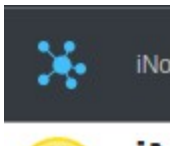


Po uruchomieniu się aplikacji pokazuje ona urządzenia, które przesyłają dane na serwer MQTT iot.inode.pl. Jest to bezpłatny testowy serwer MQTT dla użytkowników produktów **iNode**.

Ważne !

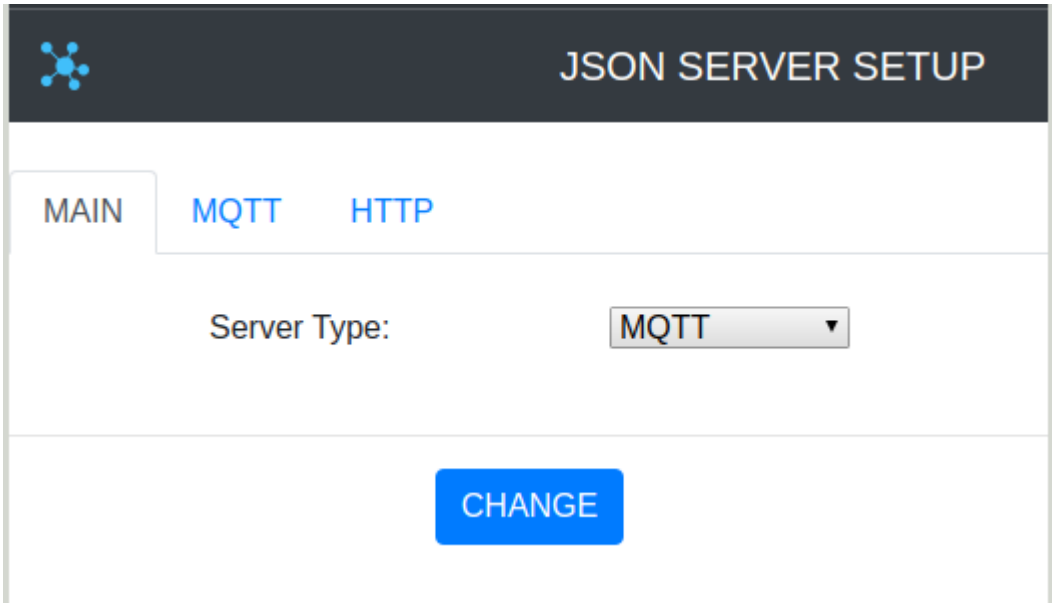
Firma ELSAT s.c. nie gwarantuje, że serwer MQTT iot.inode.pl będzie dostępny w przyszłości oraz na jakich warunkach. Użytkownik musi być świadom, że dane wysyłane na ten serwer mogą być odbierane przez innych. Dla zachowania prywatności, należy zapewnić, aby wysłane na ten serwer dane były szyfrowane – jest to opcja domyślna w **iNode LAN Central**. Domyślne hasło do ich szyfrowania jest w każdym urządzeniu inne i tworzone losowo. Dane na serwerze nie są w żaden sposób archiwizowane, są jednak publicznie dostępne co wynika ze specyfiki działania serwera MQTT jeżeli dostęp do niego nie jest ograniczony za pomocą nazwy użytkownika i hasła. Firma ELSAT s.c. w żaden sposób nie odpowiada za treść tych danych i w żaden sposób w nie nie ingeruje – moderuje.

Konfiguracja aplikacji **iNode MQTT Monitor** odbywa się po kliknięciu na obrazku w lewym górnym rogu ekranu:

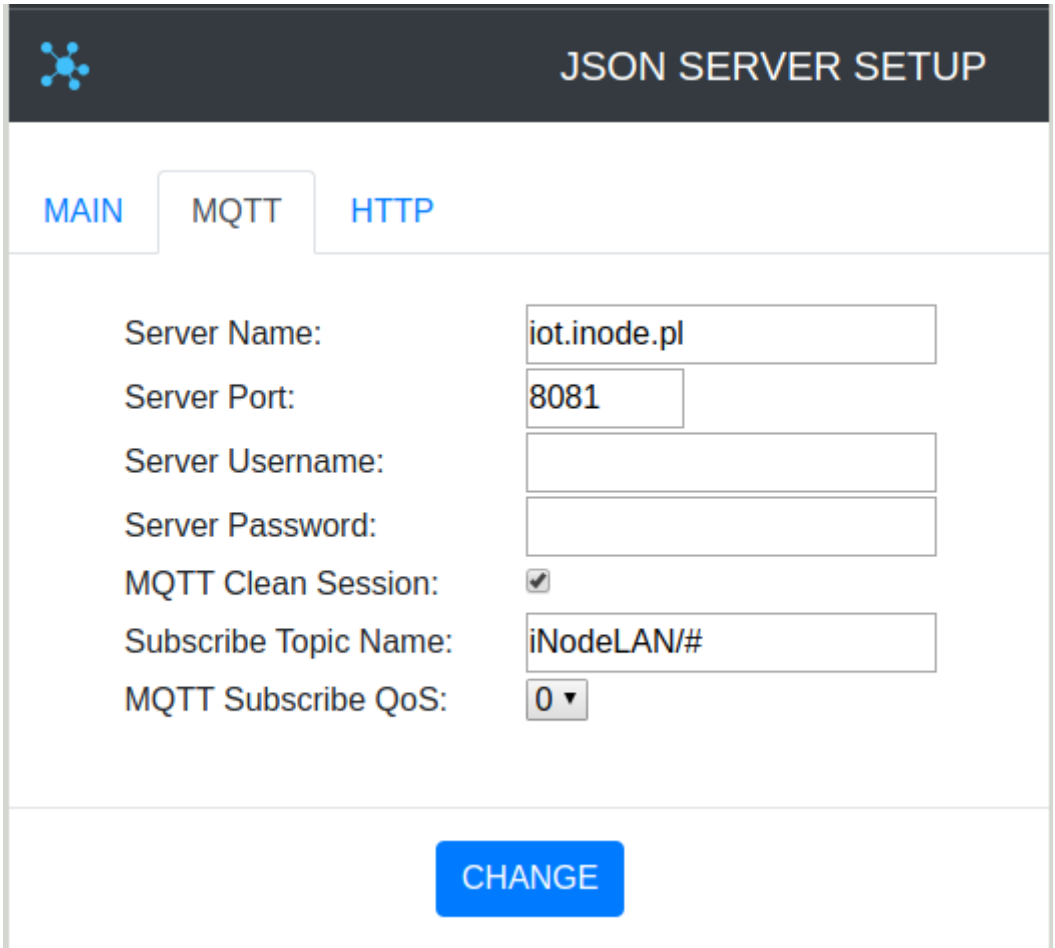


Pojawi się wtedy następujący ekran aplikacji – **JSON SERVER SETUP**:

Zakładka **MAIN** umożliwia wybranie rodzaju serwera z którym aplikacja ma współpracować. Może to być HTTP, MQTT, USB lub BLUETOOTH. Ta ostatnia opcja jest dostępna od wersji Google Chrome 79 jednak jak na razie działa tylko pod systemem Android. Może być konieczne włączenie w **chrome://flags/#enable-experimental-web-platform-features** dla USB lub BLUETOOTH.

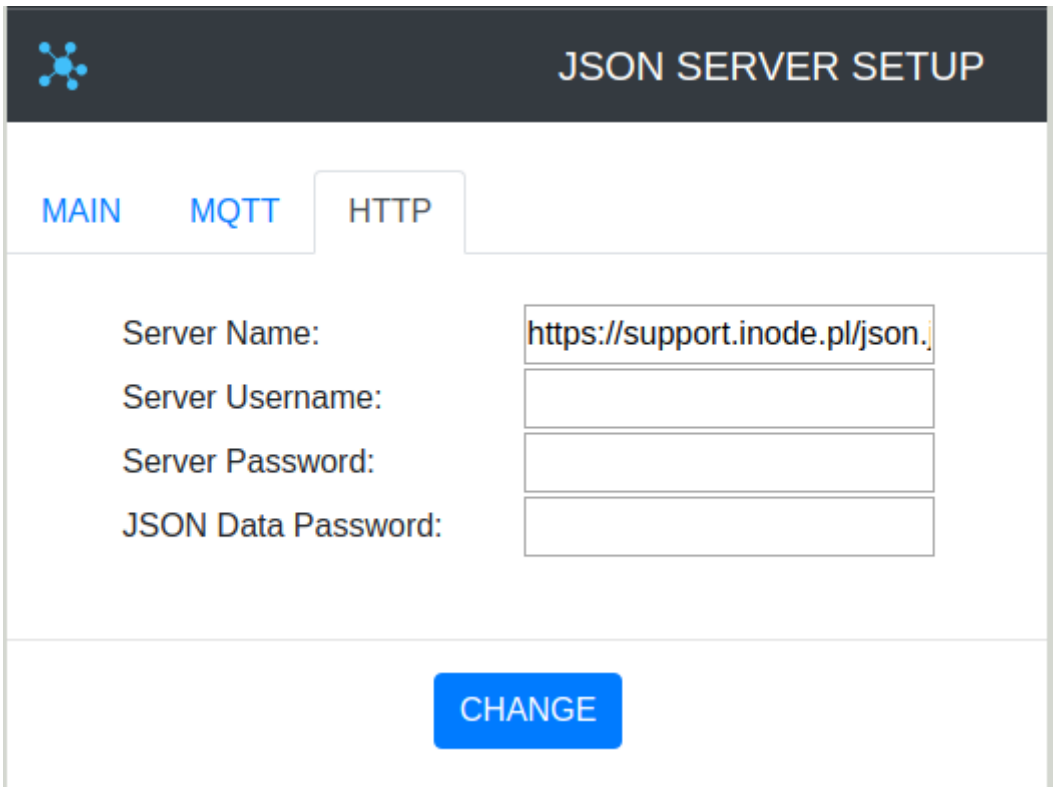


Zakładka **MQTT** umożliwia podanie parametrów serwera MQTT.



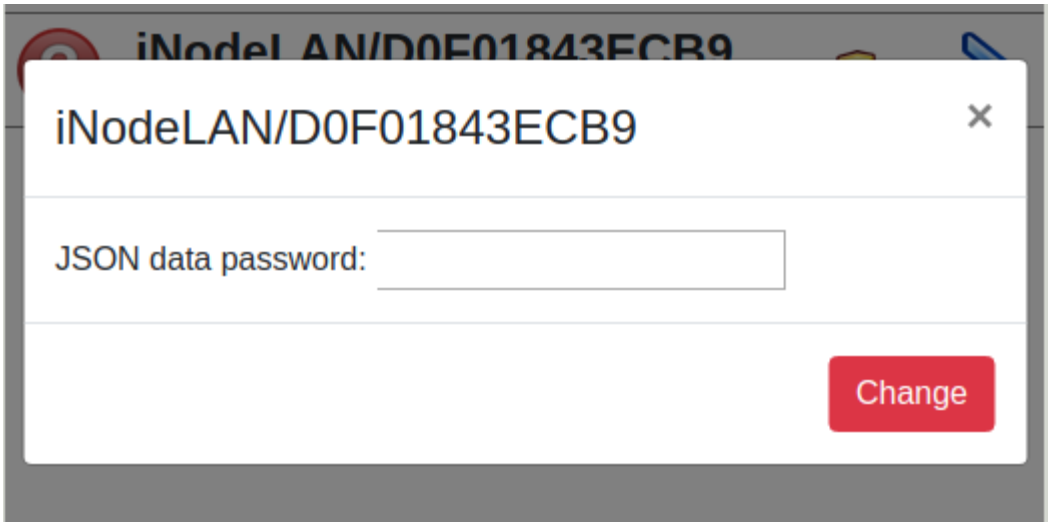
- ***Server Name*** – nazwa serwera
- ***Server Port*** – port pod którym dostępna jest usługa WebSocket serwera MQTT
- ***Server Username*** – nazwa użytkownika jeśli dostęp do serwera MQTT jest ograniczony
- ***Server Password*** – hasło dostępu do serwera MQTT
- ***MQTT Clean Session*** - gdy flaga ***MQTT Clean Session*** jest ustawiona, klient nie chce trwałej sesji. Jeśli klient rozłącza się z jakiegokolwiek powodu, wszystkie informacje i komunikaty w kolejce z poprzedniej trwałej sesji zostają utracone.
- ***Subscribe Topic Name*** – musi to być taka sama wartość jak w ustawieniach **iNode LAN Central** w polu **Page/Topic Name** lub jej fragment.
- ***MQTT Subscribe QoS:***
  - ***QoS 0*** - klient nie otrzyma od serwera żadnego potwierdzenia. Podobnie wiadomość dostarczona klientowi z serwera nie musi być potwierdzona. Jest to najszybszy sposób publikowania i odbierania wiadomości, ale także ten, w którym najprawdopodobniej nastąpi utrata wiadomości.
  - ***QoS 1*** - klient otrzyma wiadomość potwierdzającą z serwera po jej opublikowaniu. Jeśli oczekiwane potwierdzenie nie zostanie odebrane w określonym czasie, klient musi ponowić wiadomość. Wiadomość otrzymana przez klienta również musi zostać potwierdzona na czas, w przeciwnym razie serwer ponownie dostarczy wiadomość.

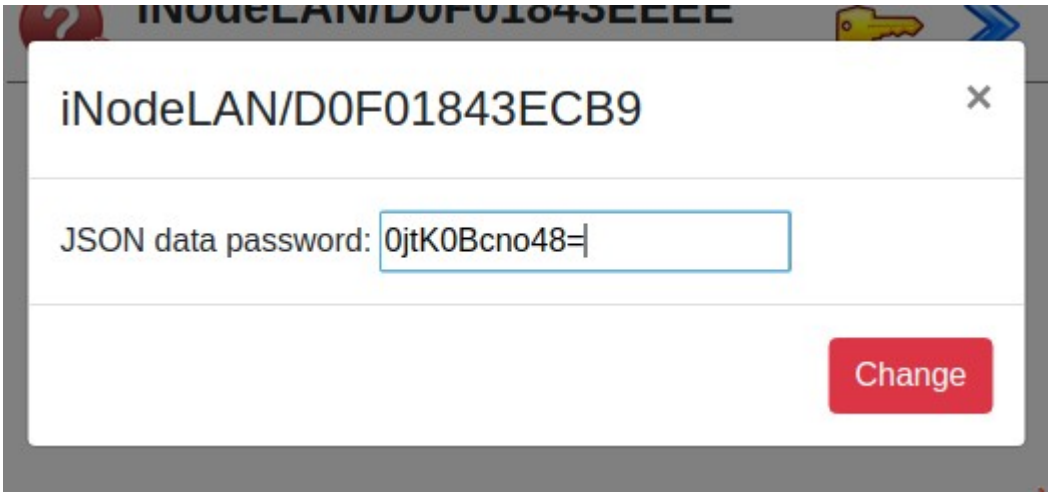
Zakładka **HTTP** umożliwia podanie parametrów serwera HTTP.



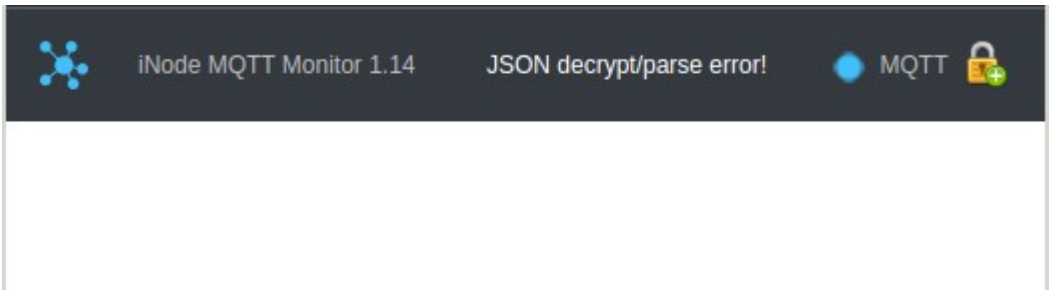
- ***Server Name*** – pełen url zawierający nazwę serwera oraz ścieżkę do pliku z danym JSON
- ***Server Port*** – port pod którym dostępna jest usługa serwera HTTP
- ***Server Username*** – nazwa użytkownika jeśli dostęp do serwera HTTP jest ograniczony. Rodzaj autoryzacji Basic.
- ***Server Password*** – hasło dostępu do serwera HTTP

Jeżeli **iNode LAN Central** przesyła dane JSON zaszyfrowane, to w aplikacji należy, po wybraniu obrazka z kluczykiem, podać hasło do ich odkodowania i nacisnąć przycisk **CHANGE**. Musi to być to samo hasło co w ustawieniach **SETUP** w polu ***JSON data password***.

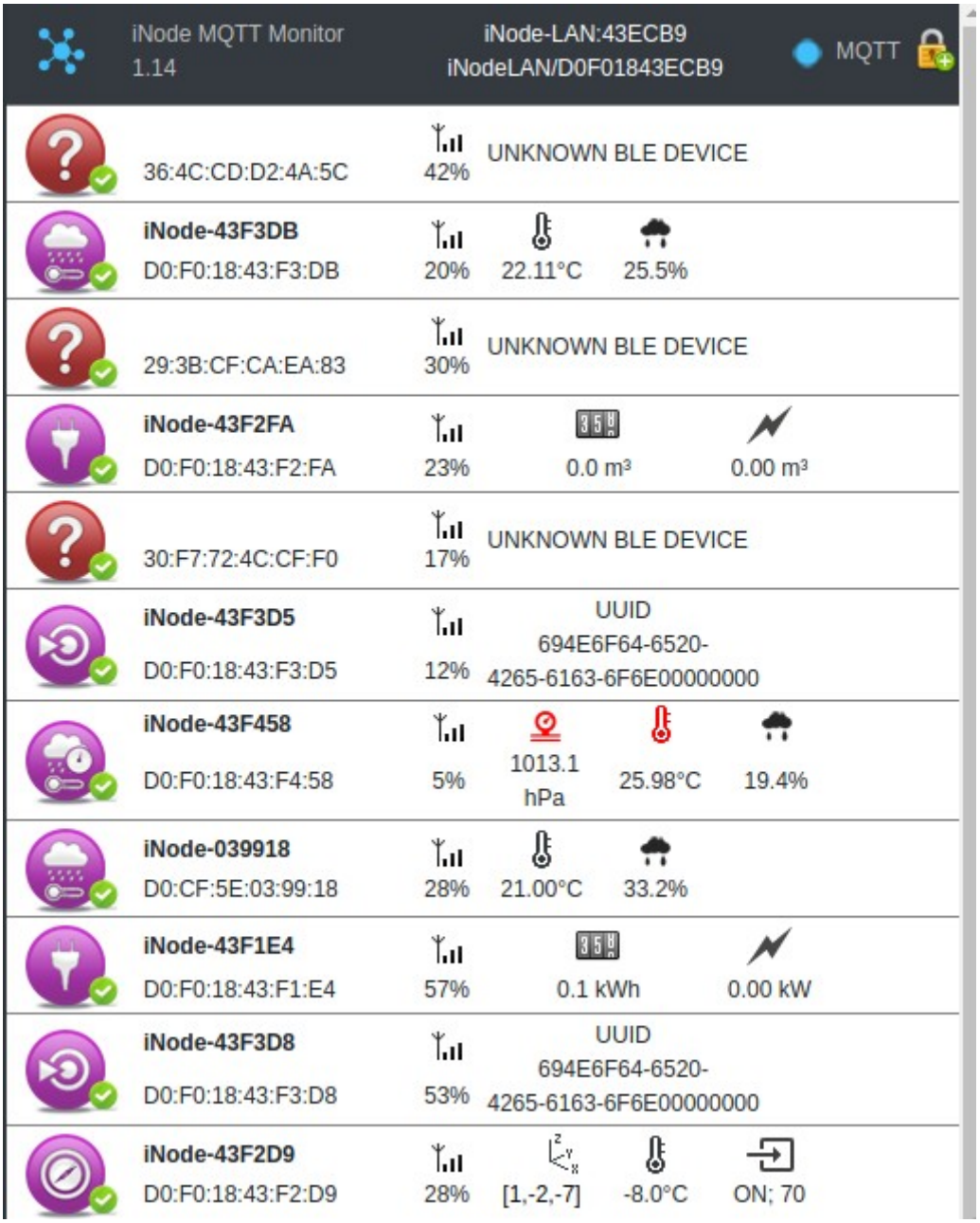




Jeżeli hasło jest nieustawione lub złe to po wybraniu niebieskiej strzałki w prawo pojawi się informacja o błędzie - ***JSON decrypt / parse error***. To, że dane są zaszyfrowane pokazuje obrazek kłódki w prawym górnym rogu ekranu.



Jeżeli hasło zostało podane prawidłowo to aplikacja wyświetli informację o urządzeniach BLE, które są wysyłane przez dany ***iNode LAN Central***. Najeżdżając myszką lub dotykając palcem poszczególnych elementów (smartfon) będą wyświetlane dodatkowe informacje o danym urządzeniu BLE.



3. Format danych JSON

3.1. Odszyfrowane dane JSON:

Na pierwszej pozycji przesyłanych danych JSON - tablicy ***data*** znajdują się informacje na temat **iNode LAN Central**.

- timestamp – znacznik czasu
- type – nazwa
- mac – adres mac
- rtc – czas urządzenia w sekundach
- ethRx – liczba ramek odebranych przez LAN
- ethTx – liczba ramek wysłana przez LAN
- bleRx- liczba ramek odebrana przez BLE
- bleTx - liczba ramek wysłanych przez BLE (tylko jeśli jest włączone skanowanie aktywne)
- workTime – czas pracy urządzenia w sekundach
- txp – ustawiona moc nadawania
- rst – liczba resetów urządzeniach
- temp – temperatura urządzenia w stopniach Celsjusza
- msg – liczba wysyłek danych JSON
- ack – liczba potwierdzonych wysyłek danych
- tx_time – czas wysyłki danych JSON w mikrosekundach
- juf – informacje o zabezpieczeniach
- period – okres wysyłania danych JSON
- manuf – kod typu urządzeniach
- rstr – przyczyna ostatniego resetu

{"data": [{"timestamp": "2020-02-05T13:10:35Z","type": "iNode-LAN:43ECB9","mac": "D0F01843ECB9","ip": "10.10.6.47","rtc": 1580908235,"ethRx": 85,"ethTx": 1,"bleRx": 114,"bleTx": 0,"workTime": 17,"txp": 8,"rst": 7,"temp": 56,"msg": 2,"ack": 1,"tx_time": 168508,"juf": 128,"period": 15,"manuf": 244,"rstr": 20},{"timestamp": "2020-02-05T13:10:34Z","mac": "D0F01843F3D8","rssi": -64,"rawData": "0201061107694E6F646520426561636F6E0000000003FF0080020A08","rawResp": "0D09694E6F64652D343346334438"},{"timestamp": "2020-02-05T13:10:35Z","mac": "35FD6890709F","rssi": -64,"rawData": "1EFF06000109200240FFC4543224734A4054BEABBFCF2DE413BBB209EC8750","rawResp": ""},{"timestamp": "2020-02-05T13:10:35Z","mac": "1DB6F43813AF","rssi": -66,"rawData": "1EFF060001092002468330 7B82213C7F54DD5BBB25CE60CE90ED7FC8E15B97","rawResp": ""},{"timestamp": "2020-02-05T13:10:34Z","mac": "FE2BD474F9EC","rssi": -57,"rawData": "031941030201060303E7FE09FFF8F8ECF974D42BFE0409503131","rawResp": ""},{"timestamp": "2020-02-05T13:10:35Z","mac": "D0F01843DB0F","rssi": -57,"rawData": "02010603FFC088020AFE0D09694E6F64652D343344423046","rawResp": ""},{"timestamp": "2020-02-05T13:10:34Z","mac": "D0F01843F3DA","rssi": -79,"rawData": "02010619FFC09B01B000000000931800000F00CCF6B00428FEE4821F30","rawResp": "0D09694E6F64652D343346334441020AFE"},{"timestamp": "2020-02-05T13:10:33Z","mac": "D0F01843F15C","rssi": -77,"rawData": "0201060EFFA0820000C31300006440B100A0020A08","rawResp": "0D09694E6F64652D343346313543"},{"timestamp": "2020-02-05T13:10:33Z","mac": "D8A01D6B8E1A","rssi": -79,"rawData": "0F0843656E7472616C2D364238453141","rawResp": ""},{"timestamp": "2020-02-05T13:10:35Z","mac": "30F7724CCFF0","rssi": -83,"rawData": "1AFF4C00021550765CB7D9EA4E2199A4FA879613A49270D8B708CE","rawResp": ""},{"timestamp": "2020-02-05T13:10:34Z","mac": "D0F01843F3DB","rssi": -84,"rawData": "02010619FF909B01C000000000471836100F0090F6D67324F4862721D3","rawResp": "0D09694E6F64652D343346334442020AFE"},{"timestamp": "2020-02-05T13:10:34Z","mac": "D0F01843F1E4","rssi": -52,"rawData": "0201060EFF908200004D000000E803B20080020AFE","rawResp": "0D09694E6F64652D343346314534"},{"timestamp": "2020-02-05T13:10:34Z","mac": "D0CF5E03930E","rssi": -66,"rawData": "0201060EFFA08200009F000000E803A00000020A14","rawResp": "0D09694E6F64652D303339333045"},{"timestamp": "2020-02-05T13:10:34Z","mac": "D0F01843E2C5","rssi": -74,"rawData": "02010619FF129D01B00004643F3519D812390034FE30FD8292C68368FC","rawResp": "0D09694E6F64652D343345324335020A06"},{"timestamp": "2020-02-05T13:10:34Z","mac": "D0F01843F2FA","rssi": -72,"rawData": "0201060EFFA0820000010000000E843B00000020AFE","rawResp": "0D09694E6F64652D343346324641"},{"timestamp": "2020-02-05T13:10:34Z","mac": "D0F01843F3D5","rssi": -74,"rawData": "0201061107694E6F646520426561636F6E0000000003FF0080020AFE","rawResp": "0D09694E6F64652D343346334435"},{"timestamp": "2020-02-05T13:10:34Z","mac": "D0F01843F2D9","rssi": -70,"rawData": "02010619FF1A9500C00000B807F81F46001B001ADC26436A4EC8AAD4CF","rawResp": "0D09694E6F64652D343346324439020A08"},{"timestamp": "2020-02-05T13:10:34Z","mac": "D0CF5E039918","rssi":

-74,"rawData": "02010619FF009BFF80000000009E1813130000A9FEC617BB7D98BD395D","rawResp": "0D09694E6F64652D303339393138"},{"timestamp": "2020-02-05T13:10:33Z","mac": "D0F01843F3DC","rssi": -79,"rawData": "02010619FF909101B00000077CA08000000F0090F605A530C80FB0D0F4","rawResp": "0D09694E6F64652D343346334443020AFE"},{"timestamp": "2020-02-05T13:10:35Z","mac": "D0F01843F150","rssi": -79,"rawData": "02010619FF149E00C000006D02A10000000900A24846D5481621C47BE9","rawResp": "0D09694E6F64652D343346313530020A08"},{"timestamp": "2020-02-05T13:10:33Z","mac": "D0F01843F458","rssi": -79,"rawData": "02010619FF129D01C000047C3FD818C80E0000163E538DEF07F9AF5D84","rawResp": "0D09694E6F64652D343346343538020AFE"},{"timestamp": "2020-02-05T13:10:34Z","mac": "0CF3EEA355A1","rssi": -74,"rawData": "02010417FF0C0300B8DC2023FEE4110FBE2000145E45041DBF000003030118","rawResp": ""}]}

3.2. Przetworzone dane JSON

3.3. Zaszyfrowane dane JSON:

W przypadku, gdy dane z **iNode LAN Central** są zakodowane na początku pliku JSON jest pole ***key***. Jest to tymczasowy klucz użyty do zaszyfrowania danych JSON. Jest on zaszyfrowany kluczem głównym wpisanym do **iNode LAN Central**. Dane są szyfrowane algorytmem ARCFour.

{"key": "33FE46D546832247CC91A8EA733D56E9","data": [Q}H/k_ {.m Z u Ö-
G z| Tw e Zn&v1 T} qE l m qq O J) };)x m n
ت+ e UC IA7 !j] + /k'ν 0Ee 3@^f[+ ">
y aK B\ 9: l Bٿ]k A 6 ћY(} w |SL_h)
j .xOLT S @
T h _O
Q1]}

3.4. Odszyfrowywanie danych JSON

Poniżej przykładowa funkcja funkcja w JavaScript dekodująca zaszyfrowane dane JSON. Plik jsaes.js jest do pobrania spod adresu: ***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;
}
```

3.5. Dekodowanie danych BLE:

Sposób kodowania danych w ramce rozgłoszeniowej BLE lub odpowiedzi na zapytanie aktywne. Informacje na temat kodów **AD Type** można znaleźć w Core_V4.0.pdf: Volume 3 Part C, Section 8.i na stronie https://www.bluetooth.org/en-us/specification/assigned-numbers/generic-access-profile

ramka rozgłoszeniowa:
02010619FF1293011000001700AB18951F485435BE5B809D6F571E40E8FE0000

020106
02 -> długość pola danych: 2 bajty
0106 -> dane
01 -> 0x01 -> EIR Data Type = 0x01 -> «Flags»
06 -> 0x06 -> EIR Data = 0x06 -> LE General Discoverable Mode (bit 1), BR/EDR Not Supported (bit 2)
19FF1293011000001700AB18951F485435BE5B809D6F571E40E8
19 -> długość pola danych: 25 bajtów
FF1293011000001700AB18951F485435BE5B809D6F571E40E8 -> dane(25 bajtów)
FF -> 0xFF -> EIR Data Type = 0xFF «Manufacturer Specific Data»
1293011000001700AB18951F485435BE5B809D6F571E40E8->
1293 -> 0x9312 -> 0x93XX identyfikator iNodeCareSensor #3; 0xXX1X wersja 1; 0xXXX2 od ostatniego odczytu pamięci minęły 24 h;

0110 -> 0x1001 type -> bit 15 do bit 12 -> zarezerwowane, bit 11 do bit 0 -> adres czujnika w grupie
0000 -> 0x0000 flags ->
SENSOR_ALARM_MOVE_ACCELEROMETER=1,
SENSOR_ALARM_LEVEL_ACCELEROMETER=2,
SENSOR_ALARM_LEVEL_TEMPERATURE=4,
SENSOR_ALARM_LEVEL_HUMIDITY=8,
SENSOR_ALARM_CONTACT_CHANGE=16
1700 -> 0x0017 value1
/* motion sensor */
0x8000 czujnik jest w ruchu (bit 15 =1)
bity 14 do 10:
składowa X położenia (wartość 5 bitowa ze znakiem) -> 0x00= 0
bity 9 do 5:
składowa Y położenia (wartość 5 bitowa ze znakiem) -> 0x00= 0
bity 4 do 0:
składowa Z położenia (wartość 5 bitowa ze znakiem) -> 0x17= -9
AB18 -> 0x18AB value2
/* temperature sensor */
Temperature= ((175.72 * Temp_Code)/65536)-46.85 [°C]
Temp_Code = 0x18AB *4 = 0x62AC = 25260
Temperature = 20,879 °C
951F -> 0x1F95 value3
/* humidity sensor */
%RH= ((125*RH_Code)/65536)-6 [%]
RH_Code = 0x1f95 *4 = 0x7e54 = 32340
%RH= 55,68 %

485435BE -> 0x5448BE35 time (znacznik czasu; liczba sekund od 01.01.1970)

5B80 9D6F 571E 40E8 -> cyfrowy podpis AES128 dla powyższych danych

ramka z odpowiedzią na zapytanie aktywne:

0D09694E6F64652D333536313441020A02000000000000000000000000000000

0D09694E6F64652D333536313441

0D -> długość pola danych: 13 bajtów

09694E6F64652D333536313441 -> dane

09 -> 0x09 -> EIR Data Type = 0x09 -> «Complete Local Name»

694E6F64652D333536313441 -> iNode-35614A

020A02

02 -> długość pola danych: 2 bajty

0A02 -> dane

0A-> 0x0A -> EIR Data Type = 0x0A -> «Tx Power Level»

02 -> 0x02 -> Tx Power Level = +2dBm

4. Parametry techniczne

Parametry radiowe:

- RX/TX:
  - BLE: 2402-2480 MHz
- moc wyjściowa (maksymalna):
  - BLE: +8dBm
- modulacja:
  - BLE: GFSK
- antena:
  - wewnętrzna PCB typu MIFA, 1,6dBi (wersja POE)
  - zewnętrzna SMA typu RP SMA MALE, 3dBi (POE SMA)

Parametry oprogramowania:

- konfigurowalne przez przeglądarkę:
  - tryb pracy BLE: AUTOSCAN
  - tryb pracy JSON: MQTT lub HTTP
  - moc z jaką urządzenie pracuje w BLE w zakresie od -18dBm do +8dBm
  - parametry sieci LAN – adres IP (stały lub przez DHCP), maska sieci, bramka, serwer DNS, serwer czasu NTP
  - nazwa urządzenia w sieci LAN i BLE
  - adres IP i port pod który wysyłane są pakiety UDP; sposób wysyłania: multicast, unicast lub broadcast jest konfigurowany automatycznie na podstawie adresu IP
  - hasło użytkownika
  - hasło administratora

Zasilanie:

- wersja **POE** lub **POE SMA**:
  - aktywne POE w standardzie IEEE 802.3af 48V DC 1W;

Obudowa:

- metalowa;
- wymiary: 81 mm x 38 mm x 22 mm (DxSxW);

Pozostałe:

- wsp. scan window/scan interval = 1 -> odbieranie danych z BLE przez 100 % czasu;
- sterowanie zdalne przez TCP/IP telnet na porcie 5500;
- możliwość zdalnej wymiany oprogramowania (przez przeglądarkę stron WWW);
- dwie diody LED: ethernet LINK i STATUS;
- serwer HTTP:
  - 2,9MB na strony HTTP (www) użytkownika i 1MB na strony HTTP (www) systemowe;
  - obsługa maksymalnie dwóch połączeń jednocześnie;
- złącze RJ-45 10Mbps/100Mbps Ethernet, 10BaseT; protokoły: ARP, SSDP, UDP, TCP/IP, DHCP, SNTP, HTTP, MQTT;
- przycisk reset (przywraca ustawienia fabryczne);
- czujnik temperatury o rozdzielczości 1°C;
- temperatura pracy: od -20 do 45°C;
- wilgotność: 35-80% RHG;
- masa: 45 g;

Wyposażenie:

- SMA antenna type RP SMA MALE, 3dBi (wersja POE SMA);

Oprogramowanie:

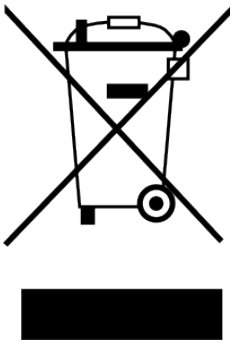
- dowolna przeglądarka stron WWW;

Chipset:

- CSR1010;
- W5500;

Producent zastrzega sobie prawo do zmiany parametrów urządzenia i oprogramowania oraz wprowadzenia innych rozwiązań konstrukcyjnych.

5. Prawidłowe usuwanie produktu (zużyty sprzęt elektryczny i elektroniczny)



Materiały z opakowania nadają się w 100% do wykorzystania jako surowiec wtórny. Utylizacji opakowania należy dokonać zgodnie z przepisami lokalnymi. Materiały z opakowania należy zabezpieczyć przed dziećmi, gdyż stanowią dla nich źródło zagrożenia. Oznaczenie umieszczone na produkcie lub w odnoszących się do niego tekstach wskazuje, że produktu po upływie okresu użytkowania nie należy usuwać z innymi odpadami pochodzącymi z gospodarstw domowych. Aby uniknąć szkodliwego wpływu na środowisko naturalne i zdrowie ludzi wskutek niekontrolowanego usuwania odpadów, prosimy o oddzielenie produktu od innego typu odpadów oraz odpowiedzialny recykling w celu promowania ponownego użycia zasobów materialnych jako stałej praktyki.

Właściwa utylizacja urządzenia:

- Zgodnie z dyrektywą WEEE 2012/19/EU symbolem przekreślonego kołowego kontenera na odpady oznacza się wszelkie urządzenia elektryczne i elektroniczne podlegające selektywnej zbiórce.Po zakończeniu okresu użytkowania nie wolno usuwać niniejszego produktu razem z normalnymi odpadami komunalnymi, lecz należy go oddać do punktu zbiórki i recyklingu urządzeń elektrycznych i elektronicznych. Informuje o tym symbol przekreślonego kołowego kontenera na odpady, umieszczony na produkcie lub w instrukcji obsługi lub opakowaniu.
- Zastosowane w urządzeniu tworzywa nadają się do powtórnego użycia zgodnie z ich oznaczeniem. Dzięki powtórnemu użyciu, wykorzystaniu materiałów lub innym formom wykorzystania zużytych urządzeń wnoszą Państwo istotny wkład w ochronę naszego środowiska naturalnego.
- Informacji o właściwym punkcie usuwania zużytych urządzeń elektrycznych i elektronicznych udzieli Państwu administracja gminna lub sprzedawca urządzenia.
- Zużyte, całkowicie rozładowane baterie i akumulatory muszą być wyrzucane do specjalnie oznakowanych pojemników, oddawane do punktów przyjmowania odpadów specjalnych lub sprzedawcom sprzętu elektrycznego.
- Użytkownicy w firmach powinni skontaktować się ze swoim dostawcą i sprawdzić warunki umowy zakupu. Produktu nie należy usuwać razem z innymi odpadami komunalnymi.

Numer Deklaracji 2/10/2019 Data wystawienia Deklaracji 10.10.2019 r.
Number of declaration of Conformity *Date of issue of declaration*

DEKLARACJA ZGODNOŚCI WE
EC DECLARATION OF CONFORMITY

My/*We*: **ELSAT s.c.**
(nazwa producenta / producer's name)
ul.Warszawska 32E/1, 05-500 Piaseczno k/Warszawy
(adres producenta / producent's address)

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

iNode LAN Central 0x0C00
POE; POE SMA;
(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:

Radio Spectrum ISM (Article 3.2 of the RED directive):
PN-ETSI EN 300 328 V2.1.1:2016-11
EMC (Article 3.1.b of the RED directive):
PN-ETSI EN 301 489-1 V2.2.0:2017-03
PN-ETSI EN 301 489-17 V3.2.0:2017-03
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

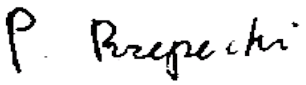
jest zgodny z postanowieniami następujących dyrektyw Unii Europejskiej:
is compatible with the following European Union directives:

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

10.10.2019 r. Paweł Rzepecki

Piaseczno k/Warszawy
(data i miejscowość / date and place)



Współwłaściciel
(podpis i stanowisko / signature and function)

RoHS 2 2011/65/EU