EMDCB

2.4 GHz Bluetooth Low Energy Motion And Illumination Sensor

Observe precautions! Electrostatic sensitive devices!

Patent protected:
WO98/36395, DE 100 25 561, DE 101 50 128,
WO 2004/051591, DE 103 01 678 A1, DE 10309334,
WO 04/109236, WO 05/096482, WO 02/095707,
US 6,747,573, US 7,019,241

REVISION HISTORY

The following major modifications and improvements have been made to this document:

Version	Author	Reviewer	Date	Major Changes
1.0	MKA	RS	14.12.2018	First public release
1.1	MKA	MKA	18.02.2018	Additional information on light sensor
1.2	MKA	MKA	07.06.2019	Added 2 Mbit mode and RPA example
1.3	MKA	MKA	06.08.2019	More detailed description of sensor functionality

Published by EnOcean GmbH, Kolpingring 18a, 82041 Oberhaching, Germany
www.enocean.com, info@enocean.com, phone +49 (89) 6734 6890

Important!
This information describes the type of component and shall not be considered as assured characteristics. No responsibility is assumed for possible omissions or inaccuracies. Circuitry and specifications are subject to change without notice. For the latest product specifications, refer to the EnOcean website: http://www.enocean.com.
As far as patents or other rights of third parties are concerned, liability is only assumed for modules, not for the described applications, processes and circuits.
EnOcean does not assume responsibility for use of modules described and limits its liability to the replacement of modules determined to be defective due to workmanship. Devices or systems containing RF components must meet the essential requirements of the local legal authorities.
The modules must not be used in any relation with equipment that supports, directly or indirectly, human health or life or with applications that can result in danger for people, animals or real value.

Recycling information
Components of the modules are considered and should be disposed of as hazardous waste.
Please use suitable recycling operators for modules, components or packaging.

TABLE OF CONTENT

1 General Description

1.1 Basic functionality

EMDCB is a ceiling-mounted motion and illumination sensor that reports its status using Bluetooth Low Energy (BLE) advertising telegrams. It enables the realization of energy harvesting wireless occupancy and light level sensors for light, building or industrial control systems communicating wit the 2.4 GHz Bluetooth Low Energy communication standard.

EMDCB uses a passive infrared (PIR) sensor to detect motion and a dedicated illumination sensor to measure the amount of ambient light.

EMDCB reports periodically (approximately every 2 minutes when no motion is detected, approximately every 1 minute when motion is detected) the latest detected motion (motion detected or no motion detected) together with the measured light level. EMDCB will report immediately if motion is detected for the first time after a period without detected motion (e.g. when a person is entering a room).

EMDCB is self-supplied via an integrated solar cell which generates the energy required for its operation. EMDCB requires 50 lux illumination for 6 hours per day directly at the solar cell which typically is equivalent 200 lux for 6 hours per day to at room level. EMDCB is fully self-powered (no batteries required) under these lighting conditions.

For cases where sufficient ambient light is not available, EMDCB provides the option to mount a CR2032 backup battery.

Radio telegrams transmitted by EMDCB are authenticated AES-128 security based on a device-unique private key and a sequence counter. This ensures integrity and authenticity of the transmitted telegrams and prevents telegram replay (retransmission of previously transmitted telegrams).

1.2 Technical data

Antenna	Integrated antenna
Output power	+ 4 dBm Configurable via NFC
Communication range (guidance only)	75 m for ideal line of sight 10 m for indoor environment (line of sight)
Communication standard	BLE Advertising
Radio frequency (min / max)	2402 / 2480 MHz
Radio channels (default)	BLE CH 37 / 38 / 39 (2402 / 2426 / 2480 MHz) Configurable via NFC
Data rate and modulation (default)	1 Mbit/s GFSK
Motion detection radius	Up to 5 m (16 ft.) when mounted 3 m (10 ft.) high
Illumination measurement range / resolution	0 … 65000 Lux / 1 Lux
Illumination measurement accuracy	+-5% at full scale
Update rate with / without detected motion	Approximately every 2 minutes / 1 minute Configurable via NFC Initial motion detection is reported immediately
User interface	LRN button Sensitivity selection switch Notification LED
Device identification	Unique 48 Bit Device ID (factory programmed) Adjustable via NFC
Security	AES128 (CBC mode) with sequence counter
Power supply	Integrated solar cell
Required illumination to sustain operation [1]	6 hours per 24 hours at 200 Lux
Charge time from empty to full charge	30 hours at 200 Lux
Charge time from empty to first transmission	10 minutes at 200 Lux
Operating time in darkness	96 hours (after full charge)
Backup power supply (optional)	CR2032
Backup battery life	
Infrequent bright light (200 lux for 2 hrs every day)	20 years
Consistent low light (65 lux for 5 hrs every day)	15 years
Total Darkness	7.5 years
Dimensions	113,2 mm L x 65,5 mm W x 30,7 mm H (4.46" L x 2.58" W x 1.21" H)

Note 1:
The required illumination of 200 Lux for sustaining operation is given for a typical operating environment (e.g. at desk level in an office). The required minimum illumination directly at the solar cell of EMDCB is 50 Lux.

1.3 Environmental conditions

Maximum Operating Temperature(1)	0 … 60°C / 32 … 140 F (indoor use only)
Recommended Operating Temperature(1)	0 … 30°C / 32 … 85 F (indoor use only)
Humidity	20% to 85% r.h. (non-condensing)

Note 1: PIR detection requires that the moving object to be detected is significantly warmer than its environment. For the case of human motion, this means that the environment needs to be significantly colder than the human body temperature of 36.5 °C / 98 F.

1.4 Packaging information

Packaging Unit	12 units
Packaging Method	Box / pallet

1.5 Ordering information

Type	Ordering Code	Frequency
EMDCB-W-EO	E6221-K515	2.4 GHz (BLE)

2 Functional Description

2.1 EMDCB Product Overview

The energy harvesting ceiling-mounted motion and illumination sensor EMDCB from EnOcean provides wireless motion and illumination sensing functionality without batteries. Power is provided by a built-in solar cell. EMDCB transmits sensor data based on the 2.4GHz Bluetooth Low Energy standard.

The outer appearance of EMDCB is shown in Figure 1 below.

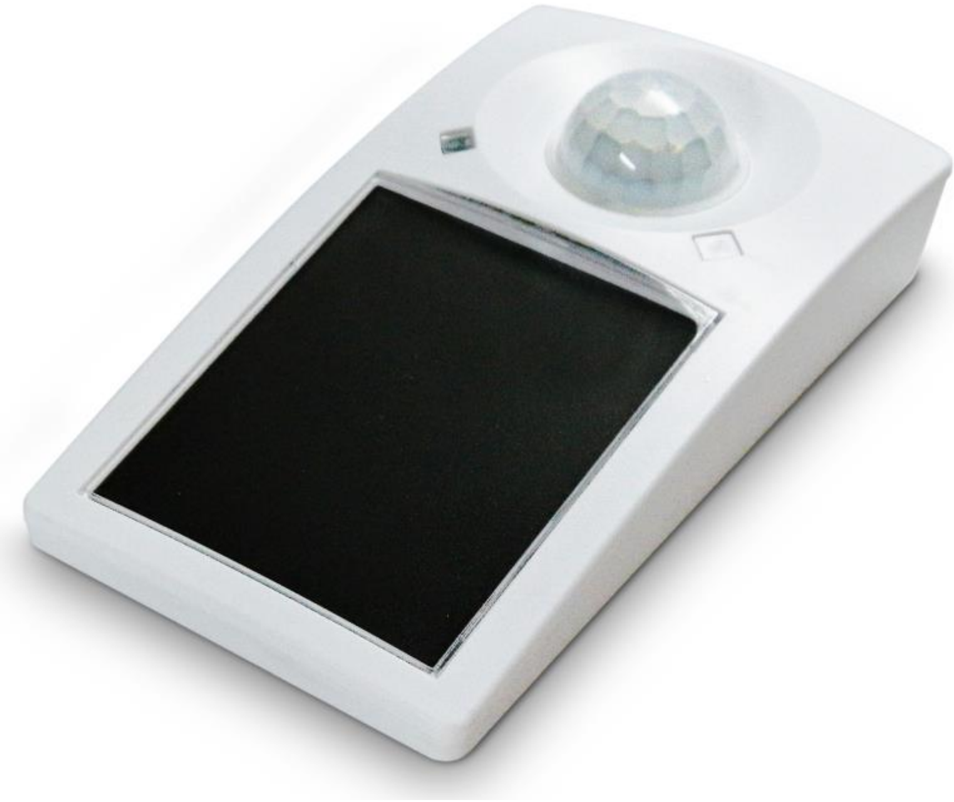


Figure 1 – EMDCB external view

2.2 Basic functionality

EMDCB devices contain a passive infrared sensor that detects changes in the received infrared radiation which are characteristic for the movement of persons.

EMDCB integrates a solar cell that generates the required energy for its operation from available ambient light.

The user interface of EMDCB consists of one button for simple configuration tasks and one LED to provide user feedback.

EMDCB is designed for ceiling mounting. It can be mounted on most ceilings with suitable screws or mounted on dropped ceilings using wire brackets.

2.3 Product design

Figure 2 below shows the EMDCB product design including key functional elements.

2.3.1 External product interface

EMDCB uses a dedicated infrared lens in conjunction with a passive infrared sensor to detect motion.

EMDCB it contains a dedicated sensor for illumination measurement. In addition, the integrated solar cell can also be used to measure the external light level. It also provides the required power for operation in normal lighting conditions.

The external user interface consists of one button (LRN) and one LED that together can be used for simple configuration and test activities.

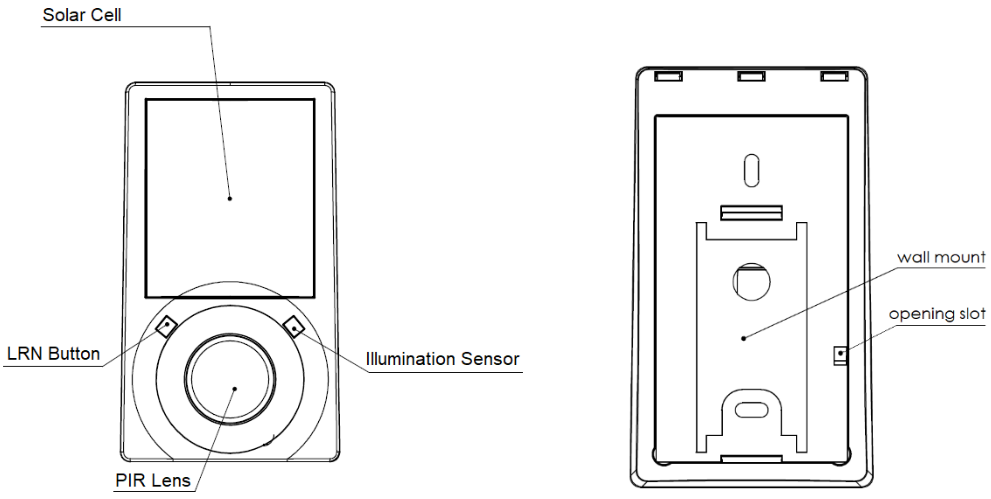


Figure 2 – EMDCB front and rear view

2.3.2 Internal product interface

EMDCB contains a holder for a CR2032 battery and a PIR sensitivity selection switch as shown in Figure 3 below.

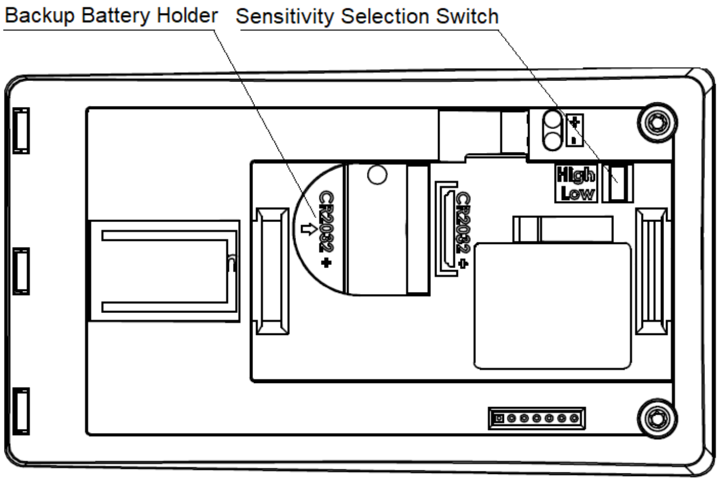


Figure 3 – EMDCB internal view

The internal product interface is accessible after removing the wall mount plate. If EMDCB has not yet been mounted onto the ceiling then the wall mount plate can be removed by using a screw driver (or similar) with the opening slot. If the EMDCB wall mount plate is already attached to the ceiling, then EMDCB can be removed by gently pulling the housing.

2.4 Functional modes

EMDCB supports three types of functional modes:

- Standard operation (shown in blue below)
- Configuration (shown in grey below)
- Standby (shown in orange below)

The transition between these modes occurs based on user action (press of the LRN button), motion detection or based on pre-defined timing intervals.

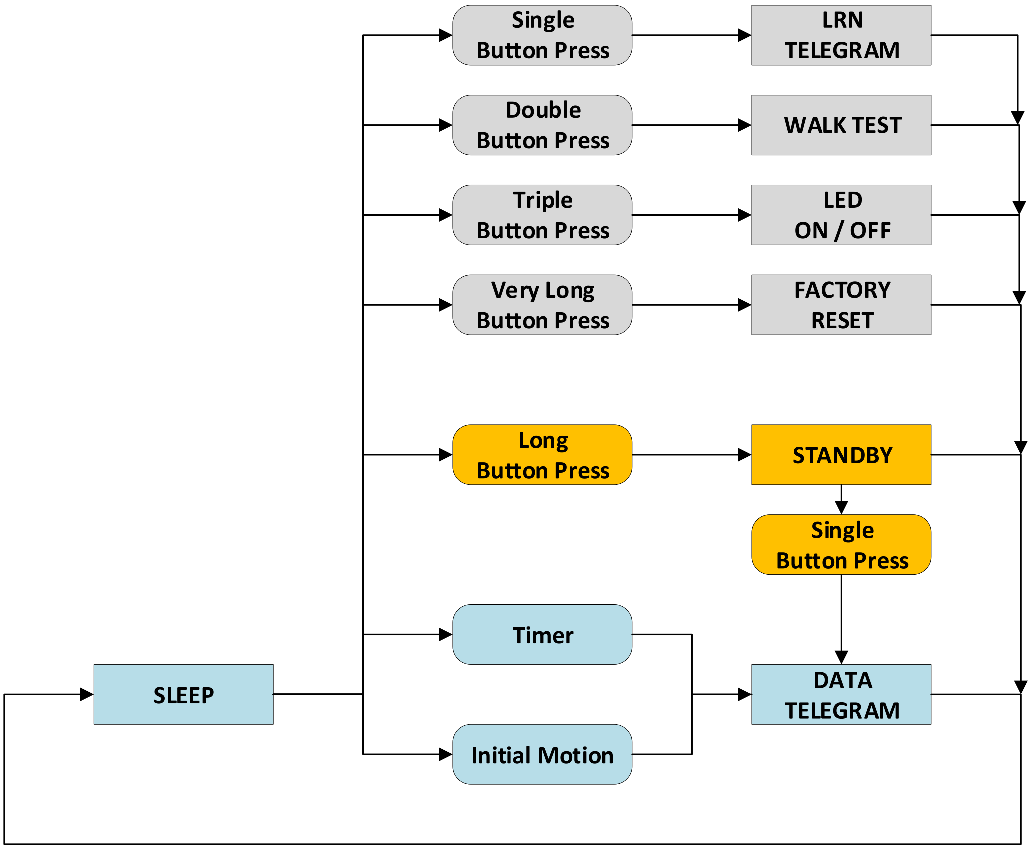


Figure 4 – EMDCB functional modes

2.4.1 Standard operation

During standard operation, EMDCB wakes up periodically and reports the current light level and motion detection status using data telegrams.

The motion detection functionality is described in chapter 2.5, the light level sensing functionality in chapter 2.6 and the data telegram transmission and format in chapters 3 and 4 respectively.

The EMDCB wake-up timer is configured to wake-up EMDCB approximately every 2 minutes during periods without detected motion and approximately every 1 minute during periods with detected motion. If motion is detected for the first time after a period without motion then EMDCB wakes up immediately.

Both the occupied and the unoccupied wake-up intervals are affected at random in order to increase the robustness of the radio transmission and to comply with regulatory requirements.

It is possible to change the wake-up intervals using the NFC interface as described in chapter 7. In case of reducing the reporting interval, the resulting increase in required energy (provided by the available light or a backup battery) has to be considered.

2.4.2 Configuration

Most EMDCB device parameters can be configured using the NFC interface as described in chapter 7. Some of the most common parameters or states can additionally be configured using the LRN button.
Table **1** below lists those.

Button Sequence	Button Timing	EMDCB Action	LED Feedback
Single Short press	< 1s	Exit from Sleep Mode if light is present Send Learn Telegram	1 short blink
Double Short Press	< 1s press, < 1s release, < 1s press	Start Walk Test (End after 2 minutes or upon next button press)	1 short blink every time movement is detected (1 second minimum interval between blinks)
Triple Short Press	< 1s press, < 1s release, < 1s press, < 1s release, < 1s press	Toggle LED indication	LED enabled: 2 short blinks LED disabled: No feedback
Long Press	3s	Enter Sleep Mode (Disable LED and Radio)	Error: No feedback Success: 3 short blinks
Very Long Press	8s	Factory Reset	Error: No feedback Success: 5 short blinks

Table 1 – EMDCB external interface actions

2.5 Motion detection

EMDCB contains an integrated passive infrared (PIR) detector that can detect moving objects based on the temperature difference between the moving object and its environment.

2.5.1 PIR detection characteristics

EMDCB is designed to detect movement within a radius of up to 5 m (16 ft.) when mounted at a ceiling of 3 m (10 ft.) height. The recommended coverage area for best detection performance is within a radius of 3 m (10 ft).

Figure 5 below shows the PIR detection pattern.

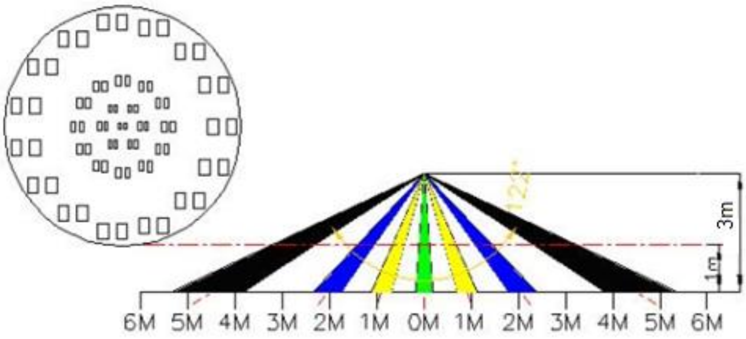


Figure 5 – EMDCB PIR detection pattern

2.5.2 Installation recommendations

Motion detection works based on the temperature difference between a moving object and its environment. Detection accuracy can therefore be affected by the following factors:

- Insufficient temperature difference (leading to no detection)
- Obstructions between PIR detector and moving person (leading to no detection)
- Warm moving objects (leading to false detections)
- Electro-magnetic radiation

For the case of person detection, the temperature of the moving object is the human body temperature (normally around 36.5 °C / 98 F). If under very hot conditions the temperature of the environment approaches the temperature of the human body, then detection performance will be significantly reduced.

For the same reason, hot objects within the detection area should be avoided. Examples include standing lights, heaters or electrical equipment generating heat.

To reliably detect motion, an unobstructed line of sight from the sensor to the person(s) in the detection area is required. Walls, room dividers, plants, book shelfs, hanging lights or other obstacles within the line of sight can limit the detection performance.

The following factors should be considered to avoid the unintended detection of other warm moving objects:

- Rapid temperature changes in the vicinity of the PIR detector, e.g. caused by fans or fan heaters being switched on or off
- Lights (especially incandescent or halogen) being switched on or off in the immediate catchment area
- Warm moving objects such as animals, machines (e.g. cleaning robots or toys), hot paper output of fax machines and laser printers, falling flower petals
- Motion in areas adjacent to the intended detection area, e.g. in the floor or in the aisle around the detection area or outside of the window

Strong external electro-magnetic fields might induce noise into the highly sensitive PIR detection circuitry and thereby affect the detection performance. EMDCB should therefore not be mounted in close vicinity of electro-magnetic radiation sources such as WiFi access points, gateways, wireless audio or video systems or other wireless devices.

For consistent detection, the mounting site of EMDCB should not be exposed to vibrations or motion.

2.6 Illumination measurement

EMDCB integrates a dedicated light level sensor used to accurately measure and report the light level directly underneath (e.g. on the desk surface).

In addition to the light sensor, EMDCB provides the option to use the calibrated solar cell response to report wide area illumination. This can be used both as input for lighting control systems (e.g. to report ambient light for daylighting applications) and to verify the available light level is sufficient for self-powered operation of EMDCB.

2.6.1 Light level sensor

EMDCB contains a dedicated humidity sensor with narrow aperture and a spectral response optimized to mimic the human eye's perception of ambient light. This light sensor reports the light level directly underneath the sensor (spot measurement).

Figure 6 shows the spectrum response of the EMDCB illumination sensor compared to that of the human eye.

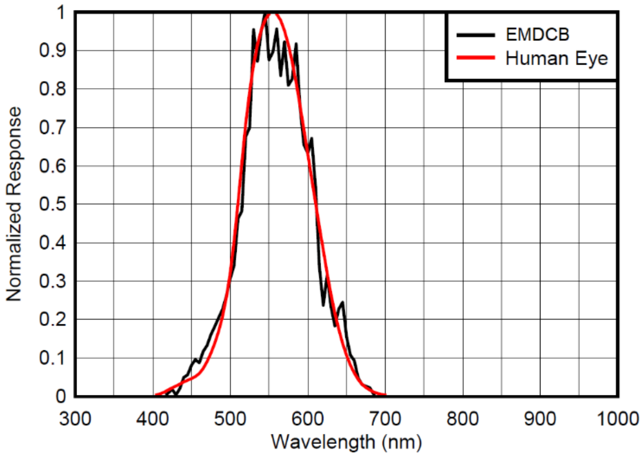


Figure 6 – Spectrum response of EMDCB illumination sensor

2.6.2 Solar cell

EMDCB can report the light level by measuring the energy generated by the solar cell. This can be used both to ensure that a sufficient ambient light is available to power the device and to measure incoming light if the solar cell is oriented towards the window. Reporting of the solar cell light level can be enabled and disabled via the NFC interface as described in chapter 7.6.8.1.

3 Radio transmission

3.1 Radio channel parameters

EMDCB transmits Bluetooth Low Energy (BLE) advertising telegrams within the 2.4 GHz radio frequency band (2402MHz … 2480MHz).

By default, EMDCB will use the three BLE advertising channels (BLE Channel 37, 38 and 39) defined for transmission. The transmission of a radio telegram on these three advertising channels is called an Advertising Event.

Use of different radio channels within the frequency band from 2402 MHz to 2480 MHz is possible using the NFC configuration interface, see chapter 7.

The initialization value for data whitening is set as follows:

- For BLE channels is set according to specification (value = radio channel)
- For the custom radio channels the initialization value is equal to the offset from 2400 MHz (e.g. value = 3 for 2403 MHz)

Table 2 below summarizes radio channels supported by EMDCB.

Radio Channel	Frequency	Channel Type
BLE Radio Channels		
37	2402 MHz	BLE Advertising Channel
0	2404 MHz	BLE Data Channel
1	2406 MHz	BLE Data Channel
…		
10	2424 MHz	BLE Data Channel
38	2426 MHz	BLE Advertising Channel
11	2428 MHz	BLE Data Channel
12	2430 MHz	BLE Data Channel
…		
36	2478 MHz	BLE Data Channel
39	2480 MHz	BLE Advertising Channel
Custom Radio Channels		
40	2403 MHz	Custom Radio Channel
41	2405 MHz	Custom Radio Channel
…		
77	2477 MHz	Custom Radio Channel
78	2479 MHz	Custom Radio Channel

Table 2 – EMDCB supported radio channels

3.2 Default radio transmission sequence

EMDCB transmits telegrams in its standard configuration by using so-called Advertising Events.

An advertising event is defined as the transmission of the same radio telegram on all selected radio channels (by default this would be on BLE Channel 37, 38 and 39) one after another with minimum delay in between.

For reliability reasons, EMDCB will send three advertising events for each reporting event. The resulting transmission sequence is shown in Figure 7 below. The default interval setting is 20 ms; an alternative setting of 10 ms can be configured via NFC (see chapter 7.6.4.2).

CHANNEL 37	CHANNEL 38	CHANNEL39	INTERVAL (20ms or 10ms)	CHANNEL 37	CHANNEL 38	CHANNEL39	INTERVAL (20ms or 10ms)	CHANNEL 37	CHANNEL 38	CHANNEL39

Figure 7 – Default radio transmission sequence

3.3 User-defined radio transmission sequences

In certain situations it might be desirable to transmit radio telegrams on channels other than the three advertising channels.

EMDCB therefore allows selecting the radio channels to be used for the transmission of data telegrams and commissioning telegrams. The following transmission modes are supported:

- Both commissioning telegrams and data telegrams are transmitted on the advertising channels as three advertising events. This is the default configuration and described in chapter 3.2 above.

- Commissioning telegrams are transmitted on the advertising channels as three advertising events while data telegrams are transmitted in a user-defined sequence as described below.

- Both commissioning and data telegrams are transmitted in a user-defined sequence as described below.

The selection of the transmission mode is done using the `TX_CHANNEL_MODE` field of the `TX` register of the NFC configuration interface as described in chapter 7.6.3.

EMDCB supports the following user-defined sequences:

- Three channel sequence
  This sequence is similar to the default Advertising Event with the difference that the user can select the radio channels to be used. The three channel sequence is described in chapter 3.3.1 below.

- Two channel sequence
  In this sequence the radio telegram is transmitted using six transmissions on two radio channels. It is described in chapter 3.3.2 below.

- One channel sequence
  In this sequence the radio telegram is transmitted using nine transmissions on one radio channel. It is described in chapter 3.3.3 below.

3.3.1 Three channel sequence

The three channel radio transmission sequence is similar to the default transmission sequence with the difference that the radio channels (BLE Channel 37, 38 and 39 in the default transmission sequence) can be selected using the registers TX_CHANNEL1, TX_CHANNEL2 and TX_CHANNEL3.

In this mode, the telegram will be transmitted on the radio channel selected by TX_CHANNEL1 first, immediately followed by a transmission on the radio channel selected by TX_CHANNEL2 and a transmission on the radio channel selected by TX_CHANNEL3.

The telegram will be transmitted using this sequence three times in total as shown in Figure 8 below.

This transmission uses a default INTERVAL setting of 20 ms; an alternative setting of 10 ms can be configured via NFC.

TX_CHANNEL1	TX_CHANNEL2	TX_CHANNEL3	INTERVAL (20ms or 10ms)	TX_CHANNEL1	TX_CHANNEL2	TX_CHANNEL3	INTERVAL (20ms or 10ms)	TX_CHANNEL1	TX_CHANNEL2	TX_CHANNEL3

Figure 8 – Three channel radio transmission sequence

3.3.2 Two channel sequence

The two channel radio transmission sequence transmits radio telegrams on two user-defined radio channels (selected by TX_CHANNEL1 and TX_CHANNEL2) six times in total.

The telegram will in this mode be transmitted on the radio channel selected by TX_CHANNEL1 first, immediately followed by a transmission on the radio channel selected by TX_CHANNEL2.

This transmission sequence uses a default INTERVAL setting of 20 ms; an alternative setting of 10 ms can be configured via NFC.

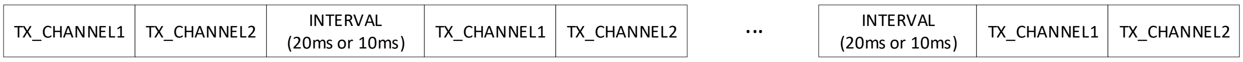


Figure 9 – Two channel radio transmission sequence

3.3.3 Single channel sequence

The single channel radio transmission sequence transmits radio telegrams on one user-defined radio channel (selected by TX_CHANNEL1) nine times in total.

This transmission sequence uses a default INTERVAL setting of 20 ms; an alternative setting of 10 ms can be configured via NFC.

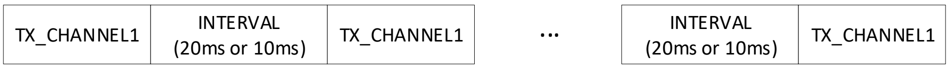


Figure 10 – Single channel radio transmission sequence

4 Telegram format

EMDCB transmits Bluetooth Low Energy (BLE) radio telegrams in the 2.4 GHz band. For detailed information about the Bluetooth Low Energy standard, please refer to the applicable specifications.

Figure 11 below summarizes the general BLE frame structure.

Preamble 0xAA	Access Address 0x8E89BED6	Header (2 Byte)	Source Address (6 Byte)	Payload (0 ... 31 Byte)	Check Sum (3 Byte)

Figure 11 – BLE frame structure

Figure 12 below shows specific properties used by EMDCB within the general BLE frame structure.

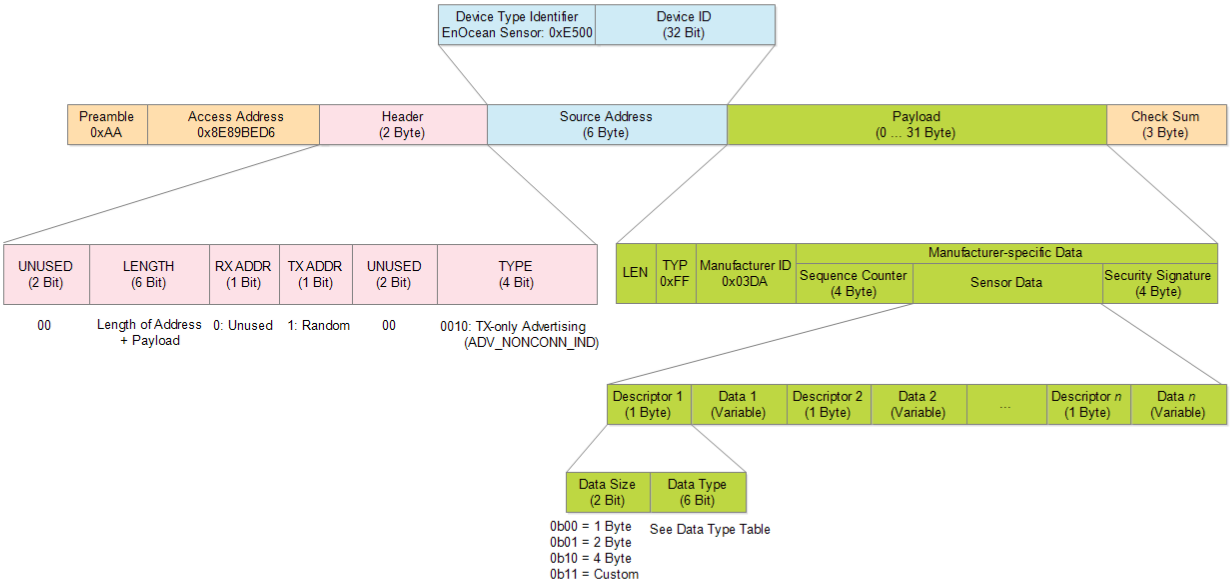


Figure 12 – BLE frame structure

The content of these fields is described in more detail below.

4.1 Preamble

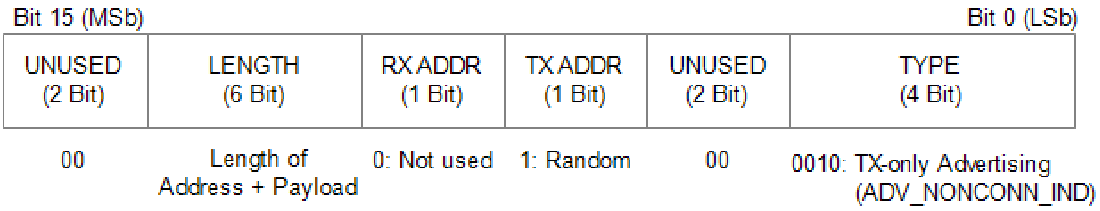
The BLE Preamble is 1 byte long and identifies the start of the BLE frame. The value of the BLE Preamble is always set to `0xAA`.

4.2 Access Address

The 4 byte BLE Access Address identifies the radio telegram type. For advertising frames, the value of the Access Address is always set to `0x8E89BED6`.

4.3 Header

The BLE Header identifies certain radio telegram parameters. Figure 13 below shows the structure of the BLE header.



Bit 15 (MSb) … Bit 0 (LSb)

UNUSED (2 Bit)	LENGTH (6 Bit)	RX ADDR (1 Bit)	TX ADDR (1 Bit)	UNUSED (2 Bit)	TYPE (4 Bit)
00	Length of Address + Payload	0: Not used	1: Random	00	0010: TX-only Advertising (ADV_NONCONN_IND)

Figure 13 – BLE header structure

4.4 Source address

The 6 byte BLE Source Address (MAC address) uniquely identifies each EMDCB product.

EMDCB supports two source address modes:

- Static Source Address mode (default)
  In this mode, the source address is constant (but its lower 32 bit can be configured via NFC interface)

- Resolvable Private Address mode (NFC configurable)
  In this mode, the source address changes for each transmission according to a pre-defined scheme

EMDCB uses by default Static Source Address mode.

Resolvable Private Address mode can be selected by setting the `ADDRESS_MODE` field in the TX_CONFIG register to 0x01 as described in chapter 7.6.7.2.

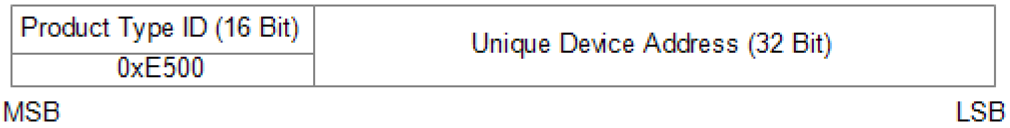
4.4.1 Static source address mode

By default, EMDCB uses static source addresses meaning that the source address is constant during normal operation. The lower 4 byte of the static source address can be configured (written) via NFC as described in chapter 7.5.

The structure of EMDCB static addresses is as follows:

- The upper 2 bytes of the source address are for EnOcean Bluetooth sensors always set to `0xE500` to enable quick identification
- The lower 4 bytes are uniquely assigned to each device. They can be read and changed using the NFC configuration interface as described in chapter 7.5.

Figure 14 below illustrates the static address structure used by EMDCB.



Product Type ID (16 Bit)	Unique Device Address (32 Bit)
0xE500	

Figure 14 – BLE static source address structure

4.4.2 Resolvable private address mode

For some applications it is desirable to modify (rotate) the source address used by EMDCB in order to prevent tracking of its radio transmissions. At the same time, each EMDCB device must remain uniquely identifiable by the receiver. To achieve these goals, EMDCB can be configured via NFC to use resolvable private addresses (RPA).

Using resolvable private addresses requires that both EMDCB and the receiver both know a common key – the so-called Identity Resolution Key (IRK). EMDCB uses its device-unique random key as identity resolution key. This key can be configured via the NFC configuration interface as described in chapter 7.5.

For resolvable private addresses, the 48 bit address field is split into two sub-fields:

- `prand`
  This field contains a random number which always starts (two most significant bits) with 0b10. The `prand` value is changed for each telegram that is transmitted. Individual advertising events used to transmit one telegram use the same `prand` value.

- `hash`
  This field contains a verification value (hash) generated from `prand` using the IRK

The structure of a random resolvable private address is shown in Figure 15 below.

<table>
<tr><td colspan="3">prand (24 Bit)</td><td rowspan="2">hash (24 Bit)</td></tr>
<tr><td>0</td><td>1</td><td>Random Data (22 Bit)</td></tr>
</table>

MSB LSB

Figure 15 – BLE private resolvable source address structure

The `prand` value is encrypted using the IRK. The lowest 24 bit of the result (encrypted value) are then used as `hash`. The concatenation of 24 bit `prand` and 24 bit `hash` will be transmitted as 48 bit resolvable private address.

The receiver maintains a list of IRK for all transmitters that are known to it (have been commissioned to work with it). Whenever it receives a radio telegram with resolvable private address (identified by the most significant bits being set to `0b10`), it will itself generate a 24 bit `hash` from the 24 bit `prand` sequentially using the IRK of each device that it has been learned into it. If an IRK matches (i.e. when `prand` is encoded with this specific IRK then the result matches `hash`), then the receiver has established the identity of the transmitter.

So conceptually the IRK takes the role of the device source address while `prand` and `hash` provide a mechanism to select the correct IRK among a set of IRK.

Figure 16 below illustrates the address resolving scheme for random private addresses.

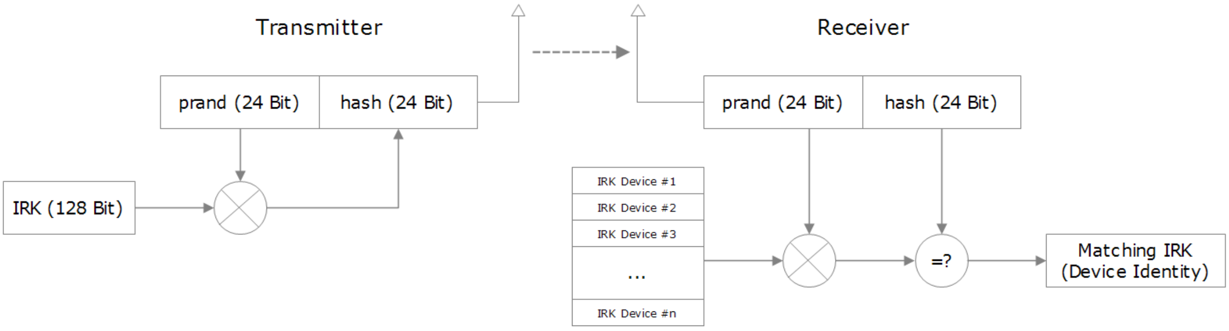


Figure 16 – Resolving private source addresses

Appendix C gives an example how to resolve a resolvable private address using a previously exchanged identity resolution key (IRK).

4.5 Check Sum

The 3 byte BLE Check Sum is used to verify data integrity of received BLE radio telegrams. It is calculated as CRC (cyclic redundancy check) of the BLE Header, Source Address and Payload fields.

4.6 Payload

The payload of EnOcean BLE sensor data telegrams can in general be up to 31 bytes long (depending on the size of the sensor data) and consists of the following fields:

- Length (1 byte)
  The Length field specifies the combined length of the following fields and depends on the size of the Sensor Status field. The minimum length is 13 byte and the maximum length is 31 byte

- Type (1 byte)
  The Type field identifies the data type used for this telegram. For STM 500B data telegrams, this field is always set to `0xFF` to designate manufacturer-specific data field

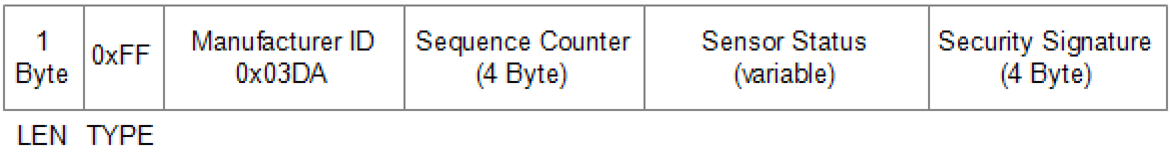
- Manufacturer ID (2 byte)
  The Manufacturer ID field is used to identify the manufacturer of BLE devices based on assigned numbers. EnOcean has been assigned `0x03DA` as manufacturer ID code.

- Sequence Counter (4 byte)
  The Sequence Counter is a continuously incrementing counter used for security processing. It is initialized to `0` at the time of production and incremented for each telegram (data telegram or commissioning telegram) sent.

- Sensor Data (variable size)
  The Sensor Data field reports the measured values of the sensors. The encoding of this field is described in chapter 4.6.1.

- Security Signature (4 byte)
  The Security Signature is used to authenticate EnOcean BLE sensor data telegrams, see chapter 5.

Figure 17 below illustrates the general telegram payload structure.



1 Byte	0xFF	Manufacturer ID 0x03DA	Sequence Counter (4 Byte)	Sensor Status (variable)	Security Signature (4 Byte)
LEN	TYPE				

Figure 17 – Telegram payload structure

4.6.1 Sensor status encoding

The Sensor Status field within the Payload data identifies the status of the connected sensors. The Sensor Status field is composed of sub-fields (one per sensor attribute).

Each sub-field consists of two items:

- Sensor Data Descriptor
  The descriptor identifies the type of the attribute and the size of the following data field
- Sensor Data
  The sensor data encodes the attribute data

Figure 18 below shows the structure of the sensor status field.

Sensor 1 Descriptor	Sensor 1 Data	Sensor 2 Descriptor	Sensor 2 Data	…	Sensor *n* Descriptor	Sensor *n* Data

Figure 18 – Sensor Status field structure

4.6.2 Sensor Data Descriptor

The Sensor Data Descriptor describes type and size of the following sensor data field. It explicitly specifies the size to ensure forward compatibility, i.e. to enable future receivers to parse sensor telegrams containing unknown data types.

The Sensor Data Descriptor structure is shown in Figure 19 below.

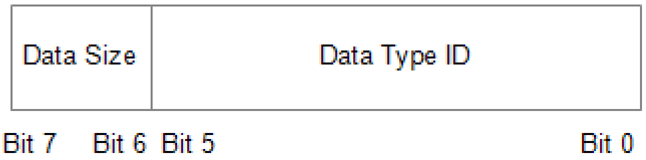


Figure 19 – Sensor Data Descriptor field structure

The sensor data descriptor explicitly specifies the data size to ensure forward compatibility for the case where an existing sensor does not "understand" subsequently introduced measurement parameters and therefore can't determine the size of their data field.

In this case, the sensor can use the length information provided by this field to determine the start of the next sensor descriptor field (which might contain usable data).

4.6.3 Data Size

The following values are possible for the Data Size field:

- 0b00 = 8 bit size (or implicit definition, e.g. commissioning telegram = 22 byte)
- 0b01 = 16 bit size
- 0b10 = 32 bit size
- 0b11 = Extended size, the size is specified in the first byte of the Sensor Data field

4.7 Supported parameters

EMDCB can report a variety of parameters. Some parameters are always reported while other parameters can be enabled and disabled via NFC.

Table 3 below summarizes the parameters that can be reported.

Standard Parameters (always reported)							
TYPE ID	Content	Size [byte]	Minimum	Maximum	Resolution	Unit	Conversion
0x05	Light level	2	0	65 533	1	lx	1 * x
0x20	Occupancy status	1	0x01 Not occupied	0x02 Occupied	Enumeration, only specified values are valid		
0x3E	Commissioning info	22	16 byte AES key followed by 6 byte advertising address				

Optional Parameters (can be enabled or disabled via NFC)								
TYPE ID	Content	Size [byte]	Default Reporting	Min	Max	Res	Unit	Conversion
0x01	Supply voltage	2	Disabled	-16383	16383	0.5	mV	2*x
0x02	Energy level	1	Enabled	0	100	0.5	%	2*x (0…200)
0x04	Solar cell light level	2	Enabled	0	65 533	1	lx	1*x
0x3C	Optional Data	Variable	Disabled	User-defined data (Size defined by *profDesc*)				

Table 3 – Supported paramters

Please refer to chapter A.1 for an example of how to parse an EMDCB data telegram and to chapter A.2 for an example how to parse a commissioning telegram.

5 EMDCB telegram authentication

EMDCB implements telegram authentication to ensure that only telegrams from senders using a previously exchanged security key will be accepted. Authentication relies on a 32 bit telegram signature which is calculated as shown in Figure 20 below and exchanged as part of the radio telegram.

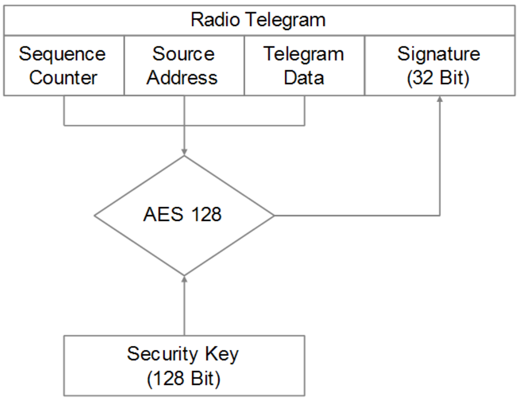


Figure 20 – Telegram authentication flow

Sequence counter, source address and the remaining telegram data together form the input data for the signature algorithm. This algorithm uses AES128 encryption based on the device-unique random security key to generate a 32 bit signature which will be transmitted as part of the radio telegram.

The signature is therefore dependent both on the current value of the sequence counter, the device source address and the telegram payload. Changing any of these three parameters will therefore result in a different signature.

The receiver performs the same signature calculation based on sequence counter, source address and the remaining telegram data of the received telegram using the security key it received from EMDCB during commissioning.

The receiver then compares the signature reported as part of the telegram with the signature it has calculated. If these two signatures match then the following statements are true:

- Sender (EMDCB) and receiver use the same security key
- The message content (address, sequence counter, data) has not been modified

At this point, the receiver has validated that the message originates from a trusted sender (as identified by its security key) and that its content is valid.

In order to avoid message replay (capture and retransmission of a valid message), it is required that the receiver tracks the value of the sequence counter used by EMDCB and only accepts messages with higher sequence counter values (i.e. not accepts equal or lower sequence counter values for subsequent telegrams).

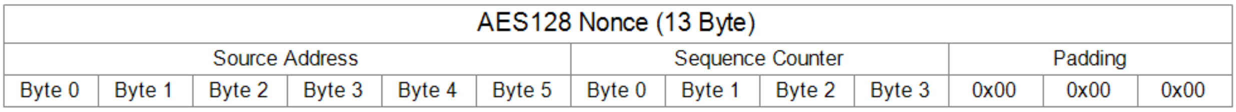
5.1 Authentication implementation

EMDCB implements telegram authentication based on AES128 in CCM (Counter with CBC-MAC) mode as described in IETF RFC3610. At the time of writing, the RFC3610 standard could be found here: https://www.ietf.org/rfc/rfc3610.txt

The 13 Byte CCM Nonce (number used once – unique) initialization value is constructed as concatenation of 6 byte Source Address, 4 byte Sequence Counter and 3 bytes of value 0x00 (for padding).

Note that both Source Address and Sequence Counter use little endian format (least significant byte first).

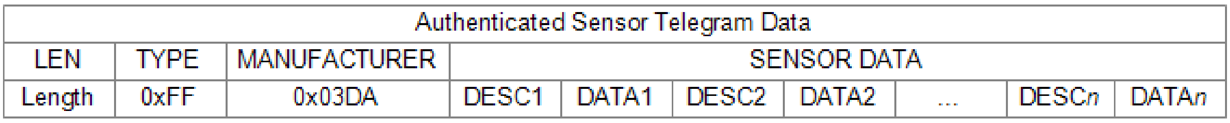
Figure 21 below shows the structure of the AES128 Nonce.



AES128 Nonce (13 Byte)												
Source Address						Sequence Counter				Padding		
Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 0	Byte 1	Byte 2	Byte 3	0x00	0x00	0x00

Figure 21 – AES128 Nonce structure

The AES128 Nonce and the 128 bit device-unique security key are then used to calculate a 32 bit signature of the authenticated telegram payload shown in Figure 22 below.



Authenticated Sensor Telegram Data									
LEN	TYPE	MANUFACTURER	SENSOR DATA						
Length	0xFF	0x03DA	DESC1	DATA1	DESC2	DATA2	…	DESC*n*	DATA*n*

Figure 22 – Authenticated payload

The calculated 32 bit signature is then appended to the data telegram payload as shown in in chapter 4.6

Appendix B gives a step by step example how to authenticate the payload of a received data telegram based on the previously exchanged security key.

6 EMDCB commissioning

Commissioning is the process by which EMDCB is learned into a receiver (actuator, controller, gateway, etc.).

The following two tasks are required in this process:

- Device identification
  The receiver needs to know how to uniquely identify this specific EMDCB device. This is achieved by using a unique 48 Bit ID (Source Address) for each EMDCB device.

- Security parameter exchange
  The receiver needs to be able to authenticate radio telegrams from EMDCB in order to ensure that they originate from this specific device and have not been modified. This is achieved by exchanging a 128 Bit random security key used by EMDCB to authenticate its radio telegrams.

EMDCB provides the following options for these tasks:

- Radio-based commissioning
  EMDCB can communicate its parameters via special radio telegrams (commissioning telegrams) to the intended receiver. Transmission of such telegrams can be triggered by using the LRN button.

- QR code commissioning
  Each EMDCB device contains an optically readable Quick Response (QR) Code which identifies its ID and its security key. This QR code can be read by a by a suitable commissioning tool (e.g. smartphone) which is already part of the network into which EMDCB will be commissioned. The commissioning tool then communicates these parameters to the intended receiver of EMDCB radio telegrams.

- NFC commissioning
  Each EMDCB device contains an NFC interface allowing to read device parameters and to configure the device.

6.1 Radio-based commissioning

Radio-based commissioning is used to associate EMDCB with other devices by sending a dedicated radio telegram (a so-called commissioning telegram).

To do so, EMDCB can transmit a dedicated commissioning telegram identifying its relevant parameters as described in chapter A.2.

The commissioning telegram will by default be transmitted on the BLE advertising channels (CH 37, 38 and 39). Use of custom radio channels is possible as described in chapter 3.3

The transmission of the commissioning telegram is triggered by pressing the LRN button.

Radio-based commissioning mode is intended for applications where NFC commissioning cannot be used. Radio-based commissioning can be disabled via NFC.

6.2 QR code commissioning

Each EMDCB device contains a product label which can be used to commission EMDC.

6.2.1 Device label

The structure of the EMDC device label is shown in Figure 23 below.

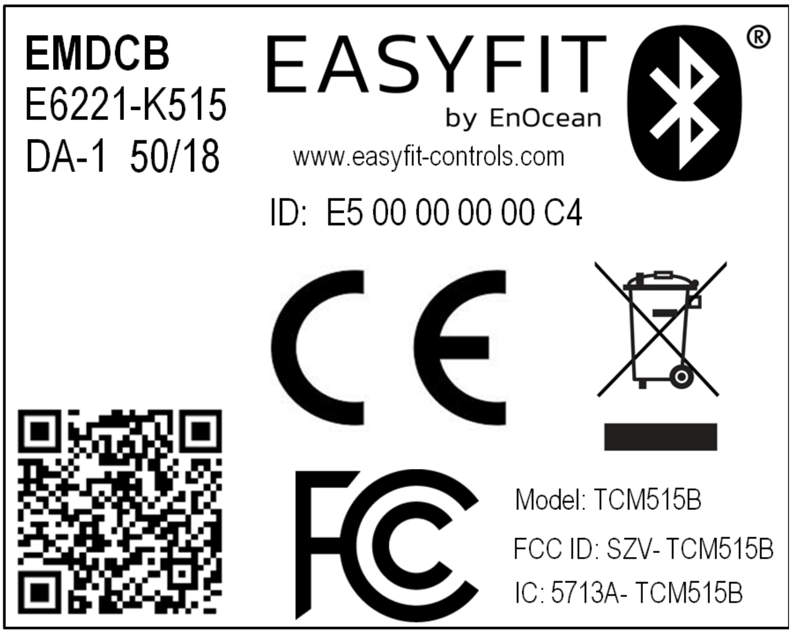


Figure 23 – EMDCB device label

6.2.2 Commissioning QR code

Each device label contains a commissioning QR code that can be scanned to identify source address and security key of EMDC to a receiver. Figure 24 shows an example of such QR code.

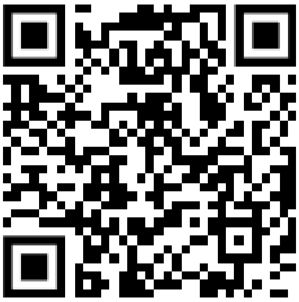


Figure 24 – EMDCB Commissioning QR code

6.2.3 Commissioning QR code format

The QR code used in the new product label encodes the product parameter according to the ANSI/MH10.8.2-2013 industry standard. The QR code shown in Figure 24 above encodes the following string:

```
30SE500000000C4+Z9E0DE9C25386B6C4F070642E19E03680+30PE6221-K515+2PDA01+S012345567890123
```

Table 4 below describes the ANSI/MH10.8.2 data identifiers used by the EMDCB device label and shows the interpretation of the data therein.

Identifier	Length of data (excluding identifier)	Value
30S	12 characters	Static Source Address (hex)
Z	32 characters	Security Key (hex)
30P	10 characters	Ordering Code (E6221-K515)
2P	4 characters	Step Code - Revision (DA-01)
S	14 characters	Serial Number

Table 4 – QR code format

From this content, it is possible to extract the device address (`E500000000C4`) and the security key (`9E0DE9C25386B6C4F070642E19E03680`) which can then be used to commission EMDCB into a receiver and to authenticate EMDCB data telegrams as described in chapter5.

6.3 Commissioning via NFC interface

EMDCB implements NFC Forum Type 2 Tag functionality as specified in the ISO/IEC 14443 Part 2 and 3 standards. This NFC functionality can be used to read the device address and the security key of EMDCB as described in chapter 7 below.

7 NFC interface

EMDCB implements an NFC configuration interface that can be used to access (read and write) the EMDCB configuration memory and thereby configure the device as described in the following chapters.

NFC communication distance is for security reasons set to require direct contact between the NFC reader and the EMDCB device.

Note that EMDCB temporarily stops operation while the NFC reader is actively connected to the NFC interface of EMDCB. EMDCB operation will automatically resume operation once the NFC reader has been disconnected.

7.1 NFC interface parameters

The NFC interface of EMDCB uses NFC Forum Type 2 Tag functionality as specified in the ISO/IEC 14443 Part 2 and 3 standards. It is implemented using an NXP NT3H2111 Mifare Ultralight tag.

7.2 NFC access protection

Protected data access is only possible after unlocking the configuration memory with the correct 32 bit PIN code. By default, the protected area is locked and the default pin code for unlocking access is `0x0000E500`.

The default pin code shall be changed to a user-defined value as part of the installation process. This can be done by unlocking the NFC interface with the old PIN code and then writing the new PIN code to page `0xE5`.

7.3 Using the NFC interface

Using the NFC interface requires the following:

- NFC reader (either PC with USB NFC reader or suitable Android smartphone)
- NFC SW with read, write, PIN lock, PIN unlock and PIN change functionality

7.3.1 USB NFC Reader

For PC applications, EnOcean recommends the TWN4 Multitech 2 HF NFC USB Reader with CDC interface from Elatec RFID Systems:
https://www.elatec-rfid.com/fileadmin/Files/Data_Sheets/DS_TWN4_MultiTech.pdf

This reader is shown in Figure 25 below.

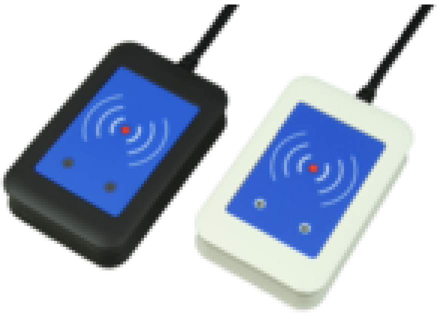


Figure 25 – Elatec TWN4 MultiTech Desktop NFC Reader with CDC interface

For additional information and support please contact sales-rfid@elatec.com.

7.3.2 Android Smartphones with NFC

NFC functionality is available in certain Android smartphones (e.g. Samsung Galaxy S7 / S8 / S9 / S10).

NXP provides a SW framework that can be used as starting point for the development of NFC configuration apps on Android devices and can advise regarding suitable tablets and smartphones.

7.4 NFC interface functions

For a detailed description about the NFC functionality, please refer to the ISO/IEC 14443 standard.

For specific implementation aspects related to the NXP implementation in NT3H2111, please refer to the NXP documentation which at the time of writing was available under this link:

http://cache.nxp.com/documents/data_sheet/NT3H2111_2211.pdf

The following chapters summarize the different functions for reference purposes.

7.4.1 NFC interface state machine

Figure 26 below shows the overall state machine of the NFC interface.

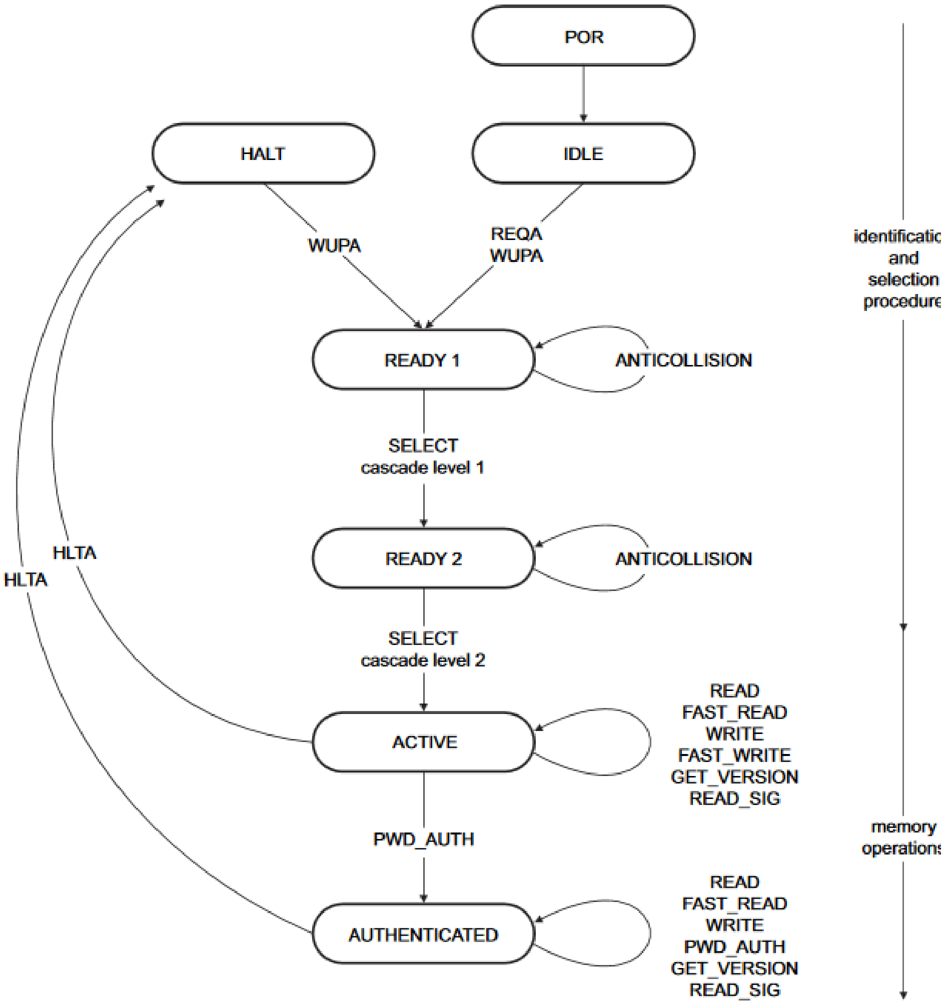


Figure 26 – NFC interface state machine

7.4.2 IDLE state

IDLE is the waiting state after a Power-On Reset (POR), i.e. after the NFC tag has been introduced into the magnetic field of the NFC reader.

The NFC tag exits the IDLE state towards the READY 1 state when either a REQA or a WUPA command is received from the NFC reader. REQA and WUPA commands are transmitted by the NFC reader to determine whether any cards are present within its working range.

Any other data received by the NFC tag while in IDLE state is discarded and the NFC tag will remain in IDLE state.

7.4.3 READY 1 state

READY 1 is the first UID resolving state where the NFC tag resolves the first 3 bytes of the 7 byte UID using the ANTICOLLISION or SELECT commands for cascade level 1.

READY 1 state is exited after the SELECT command from cascade level 1 with the matching complete first part of the UID has been executed. The NFC tag then proceeds into READY 2 state where the second part of the UID is resolved.

7.4.4 READY 2 state

READY 2 is the second UID resolving state where the NFC tag resolves the remaining 4 bytes of the 7 byte UID using the ANTICOLLISION or SELECT commands for cascade level 2.

READY 2 state is exited after the SELECT command from cascade level 2 with the matching complete part of the UID has been executed. The NFC tag then proceeds into ACTIVE state where the application-related commands can be executed.

7.4.5 ACTIVE state

ACTIVE state enables read and write accesses to unprotected memory.

If access to protected memory is required then the tag can transition from the ACTIVE state to AUTHENTICATED state by executing the PWD_AUTH command in conjunction with the correct 32 bit password.

7.4.6 Read command

The READ command requires a start page address, and returns the 16 bytes of four NFC tag pages (where each page is 4 byte in size).

For example, if the specified address is `03h` then pages `03h`, `04h`, `05h`, `06h` are returned. Special conditions apply if the READ command address is near the end of the accessible memory area.

Figure 27 below shows the read command sequence.

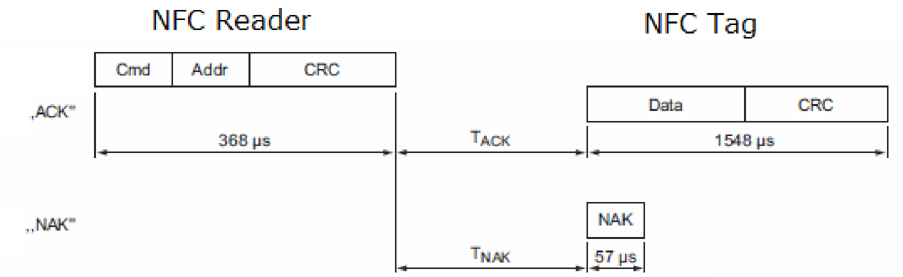


Figure 27 – NFC read command sequence

7.4.7 Write command

The WRITE command requires a start page address and returns writes 4 bytes of data into that page.

Figure 28 below shows the read command sequence.

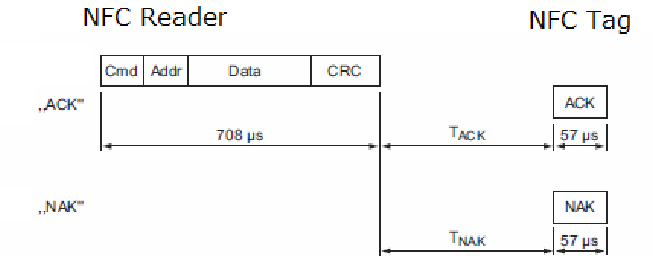


Figure 28 – NFC write command sequence

7.4.8 Password authentication (PWD_AUTH) command

The protected memory area can be accessed only after successful password verification via the PWD_AUTH command.

The PWD_AUTH command takes the password as parameter and, if successful, returns the password authentication acknowledge, PACK.

Figure 29 below shows the password authentication sequence.

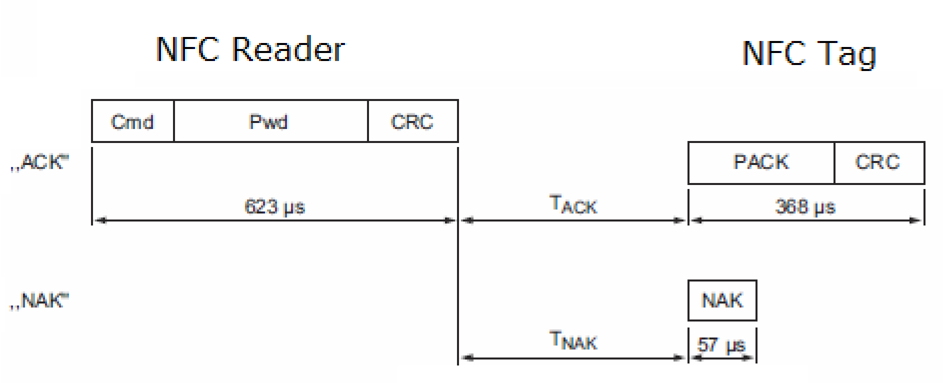


Figure 29 – Password authentication sequence

7.5 Configuration memory organization

The EMDCB configuration memory is divided into the following areas:

- Public data
- Protected data

In addition to that, EMDCB maintains a private configuration memory region used to store default parameters and confidential information which is not accessible to the user. The following chapters provide information on key settings available via NFC.

The smallest access unit is one page of 4 byte. If less than a full page (i.e. less than 4 byte) shall be written to NFC memory then the whole page should be read, its content be modified as needed and the result be written back.

7.5.1 Changing the PIN code

After successful authentication, the password can be changed by writing the new password to memory page `0xE5`.

Note that a read access to page `0xE5` always return `0x00000000`, i.e. it is not possible to read out the current PIN code.

7.6 NFC memory map

The EMDCB NFC configuration memory is divided into the following three areas:

- Public read-only data
- Private read / write data (PIN protected)
- Private read-only data (PIN protected)

The smallest access unit is one page of 4 byte. If less than a full page (i.e. less than 4 byte) shall be written to NFC memory then the whole page should be read, modified as needed and the result be written back.

The organization of the NFC configuration memory is shown in Table 5 below.

Address	Byte Offset				NFC Access
(Hex)	0	1	2	3	
00	NFC Parameters				Public Read
…					
03					
04	NDEF Text Field				
…					
1A					
1B	Internal Parameters				
…					
3B					
3C	Calibration Data				Private Read
…					
3F					
40	SOURCE_ADDRESS				Private Read / Write
41	TX_CHANNEL1	TX_CHANNEL2	TX_CHANNEL3	TX_CHANNEL_MODE	
42	TX_POWER	TX_TIMING	MANUFACTURER_ID		
43	OPTIONAL_DATA_CONTENT				
44	SECURITY_KEY (all zeros if disabled in SECURITY_CONFIG)				
…					
47					
48	KEY_ACCESS	MAC_ROTATION	LRN_ENABLE	SECURITY_MODE	
49	REPORT_CFG	OPTIONAL_DATA_SIZE	LED_MODE	RFU	
4A	TX_INTERVAL_UNOCCUPIED		TX_INTERVAL_OCCUPIED		
4B	LOW_POWER_MODE	RFU			
4C	RFU				
…					
5F					
60	Internal Data				
…					
EB					

Table 5 – NFC Memory Map

7.6.1 NDEF Text field

The NFC interface of each EMDCB device contains an NDEF Text Field that can be read with standard NFC reader. The NDEF text field encodes the same string as the QR code, see chapter 6.2.

7.6.2 Source Address

Each EMDCB device has been assigned a default 6 byte address (Static Source Address) during production. The two MSB are always 0xE500; the four LSB of this static source address can be read and modified via the NFC interface as shown in Table 6 below.

Static Source Address			
Access	Protection	Page	Remarks
R/W	PIN Protected	0x40	Byte [0:4] Lower 4 byte of source address (Upper 2 byte are always 0xE500)

Table 6 – Static Source Address

7.6.3 TX Channel Configuration

EDMCB allows users to modify the radio channels used for the transmission of its radio telegrams as described in chapter 3.3 using the TX Channel Configuration page of the NFC interface as shown in Table 7 below.

TX Channel Configuration			
Access	NFC Memory Area	Address	Remarks
R/W	PIN Protected	0x41	Byte [0] TX_CHANNEL1 (Default: 0x25 = CH37) Byte [1] TX_CHANNEL2 (Default: 0x26 = CH38) Byte [2] TX_CHANNEL3 (Default: 0x27 = CH39) Byte [3] TX_CHANNEL_MODE (Default: 0x00)

Table 7 – TX Channel Configuration

7.6.3.1 TX Channel Mode

The TX_CHANNEL_MODE register is used to select custom transmission sequences by setting the CHANNEL_MODE_SELECTION bit field shown in Figure 30 according to the desired custom radio channel mode

TX Channel Mode (Default = 0x00)							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RFU				CHANNEL_MODE_SELECTION			

Figure 30 – TX Channel Mode register structure

Table 8 below shows the encoding of the CHANNEL_MODE_SELECTION bit field for the supported custom transmission sequences.

Setting	Transmission Sequence
0b0000 (Default)	Commissioning and data telegrams in standard Advertising Mode
0b0001	Commissioning telegrams in standard Advertising Mode Data telegrams on 3 user-defined radio channels
0b0010	Commissioning telegrams in standard Advertising Mode Data telegrams on 2 user-defined radio channels
0b0011	Commissioning telegrams in standard Advertising Mode Data telegrams on 1 user-defined radio channel
0b0100	Commissioning and Data telegrams on 3 user-defined radio channels
0b0101	Commissioning and Data telegrams on 2 user-defined radio channels
0b0110	Commissioning and Data telegrams on 1 user-defined radio channel
0b011…0b1111	Unused, will be treated as 0b0000

Table 8 – Transmission Channel settings

7.6.4 Radio Configuration

The Radio Configuration page allows the user to select the transmission power, the advertising interval and the Manufacturer ID used to transmit the sensor data.

EMDCB by default uses the Bluetooth SIG manufacturer ID `0x03DA` (EnOcean GmbH) and transmits with +4 dBm output power and 20 ms advertising interval. These settings can be configured using the Transmission Settings as shown in Table 9 below.

Radio Configuration			
Access	Protection	Page	Remarks
R/W	PIN Protected	0x42	Byte [0] TX Power Byte [1] Advertising Interval Byte [2:3] Manufacturer ID

Table 9 – Radio Configuration

7.6.4.1 TX Power

EMDCB by default uses a transmission power of +4 dBm. In order to save energy, it is possible to reduce this to 0 dBm using the TX Power bit field shown in Figure 31 below.

TX Power (Default: 0x00)							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RFU						TX Power	

0b00: +4 dBm
0b01: 0 dBm
Others: Reserved

Figure 31 – TX Power register structure

7.6.4.2 Advertising Interval

EMDCB by default uses an advertising interval of 20 ms.

In order to minimize latency (especially in dual-channel and single channel transmission modes), it is possible to reduce this interval to 10 ms using the Advertsising Interval regis-rer shown in Figure 32 below.

ADVERTISING INTERVAL (Default: 0x00)							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RFU						ADVERTISING INTERVAL	

0b00: 20 ms Interval
0b01: 10 ms Interval
Others: Reserved

Figure 32 – Advertising Interval register structure

7.6.4.3 Manufacturer ID

EMDCB by default transmits using the Manufacturer ID `0x03DA` (EnOcean GmbH).

It is possible to set a different manufacturer ID using the Manufacturer ID bit field shown in Figure 33 below.

Manufacturer ID (Default: 0x03DA)				
Bit 15	Bit 14	…	Bit 1	Bit 0
MANUFACTURER ID				

0x03DA: EnOcean GmbH

Figure 33 – Manufacturer ID register structure

7.6.5 Optional Data

EMDCB allows transmitting up to four byte of optional data that can be freely defined by the user. The length of transmitted optional data is set using the OPTIONAL_DATA_SIZE register as described in chapter 7.6.8.2.

The following data will be used depending on the selected length of optional data:

- If length of Optional Data is set to 1 byte then Data Byte 0 will be transmitted
- If length of Optional Data is set to 2 byte then Data Byte 0 will be transmitted first followed by Data Byte 1
- If length of Optional Data is set to 2 byte then Data Byte 0 will be transmitted first followed by Data Byte 1, Data Byte 2 and finally Data Byte 3

The organization of the Optional Data register is shown in Table 10 below.

Optional Data			
Access	NFC Memory Area	Page	Remarks
R/W	PIN Protected	0x43	Byte [0]: Optional Data Byte 0 Byte [1]: Optional Data Byte 1 Byte [2]: Optional Data Byte 2 Byte [3]: Optional Data Byte 3

Table 10 – Optional Data register

7.6.6 Security Key

The security key used by EMDCB can be read and modified via the NFC interface as shown in Table 11 below.

Security Key			
Access	NFC Memory Area	Page	Remarks
R/W	PIN Protected	0x44 … 0x47	128 bit security key Read access to security key can be disabled using the Security Configuration register. Read returns all 0's if key access is disabled

Table 11 – Security Key register

7.6.7 Security Configuration

The security configuration of EMSB can be used to restrict access to the security key, to select the MAC Address Mode and to select the Security Mode. The structure of this register is shown in in **Fehler! Verweisquelle konnte nicht gefunden werden.** below.

SECURITY CONFIGURATION			
Access	NFC Memory Area	Page	Remarks
R/W	PIN Protected	0x48	Byte [0]: Security Key Access Byte [1]: Address Mode Byte [2]: LRN Telegram Byte [3]: Security Mode

Table 12 – Security Configuration register address

7.6.7.1 Security Key Access

Access to the security key can be restricted using the Key Access bit field as shown in Table 13 below. It is possible to require Pin input to read the security key or to disable access to the security key altogether.

Setting	**Key Access**
`0x00 (Default)`	Key read without PIN (key visible in NDEF and private area)
`0x01`	Key read with PIN (key visible only in private area)
`0x02`	Key read disabled (key not visible, write-only mode)
`0x03 … 0xFF`	Unused, will be treated as `0x00`

Table 13 – Key Access settings

7.6.7.2 Address Mode

EMSB supports two address modes:

- Static Source Address mode
  Static Source Address is set in the factory and remains the same during the lifetime of the device unless it is changed using the Source Address configuration feature described in chapter 7.6.2.

- Resolvable Private Address
  In this mode, the address used by EMDCB is changed for each radio telegram transmission as described in chapter 4.4.2

The options for the Address Mode bit field are shown in Table 14 below.

Setting	**Address Mode**
`0x00 (Default)`	Static Source Address
`0x01`	Resolvable Private Address
`0x02 … 0xFF`	Unused, will be treated as `0x00`

Table 14 – Address Mode settings

7.6.7.3 LRN Telegram

EMDCB can transmit a commissioning (LRN) telegram as described in chapter 6.1 upon press of the LRN button. The transmission of such commissioning telegram can be disabled using the LRN Telegram field shown in Table 15 below.

Setting	**LRN Telegram**
`0x00 (Default)`	LRN Telegram enabled
`0x01`	LRN Telegram disabled
`0x02 … 0xFF`	Unused, will be treated as `0x00`

Table 15 – LRN Telegram settings

7.6.7.4 Security Mode

EMDCB supports 32 bit CMAC authentication with 32 bit Sequence Counter as described in chapter 5.

Setting	**Security Mode**
`0x00 (Default)`	32 bit CMAC with 32 Bit Sequence Counter
`0x01 … 0xFF`	Unused, will be treated as `0x00`

Table 16 – Security Mode settings

7.6.8 Attribute Reporting, Optional Data Size and LED Intensity

EMDCB allows the configuration of which optional attributes are reported, how much optional data is reported and how bright the LED is illuminated. Table 17 below shows the field structure used to configure these settings.

Attribute Reporting, Optional Data Size and LED Intensity			
Access	NFC Memory Area	Page	Remarks
R/W	PIN Protected	0x49	Byte [0] ATTRIBUTE_REPORTING_CONFIG Byte [1] OPTIONAL_DATA_SIZE Byte [2] LED_INTENSITY Byte [3] RFU

Table 17 – Attribute Reporting, Optional Data Size and LED Intensity

7.6.8.1 Attribute Reporting

Figure 34 below shows how to configure the attribute reporting. By default, solar cell illumination and energy level are reported in order to determine installation conditions with insufficient light. The supply voltage is not reported by default.

ATTRIBUTE_REPORTING_CONFIG (Default: 0x06)					
Bit 7	…	Bit 3	Bit 2	Bit 1	Bit 0
Reserved		Reserved	Solar Cell Illumination	Energy Level	Supply Voltage
			0b0: Not reported	0b0: Not reported	**0b0: Not reported**
			0b1: Reported	**0b1: Reported**	0b1: Reported

Figure 34 – Attribute Reporting Field structure

7.6.8.2 Optional Data Size

The length of optional data (0, 1, 2 or 4 byte) can be selected using the OPTIONAL_DATA_SIZE field. By default, no optional data is transmitted. Optional data to be transmitted will be taken from the OPTIONAL_DATA_0 … OPTIONAL_DATA_3 bit fields (in that order) of the OPTIONAL_DATA register shown in Figure 35 below.

OPTIONAL_DATA_SIZE (Default: 0x00)				
Bit 7	…	Bit 2	Bit 1	Bit 0
Reserved		Reserved	Optional Data Size	
			0b00: No optional data	
			0b01: 1 byte optional data	
			0b10: 2 byte optional data	
			0b11: 4 byte optional data	

Figure 35 – Optional Data Size field structure

7.6.8.3 LED Intensity

The LED intensity can be controlled the LED_NOTIFICATION field shown in Figure 36 below.

LED_INTENSITY (Default: 0x02)				
Bit 7	…	Bit 1	Bit 1	Bit 0
Reserved		Reserved	LED Intensity	
			0b00: Off	
			0b01: Low intensity	
			0b10: Medium intensity	
			0b11: Maximum Intensity	

Figure 36 – LED Intensity field structure

7.6.9 Reporting interval

EMDCB allows setting the reporting interval (interval between two telegram transmissions) both for the case when motion has been detected and for the case where not motion has been detected.

By default, EMDCB will report its status approximately once every 60 seconds as long as motion is detected and approximately once every 120 seconds if no motion has recently been detected.

Note that EMDCB will report the first motion detection (when a previously unoccupied area becomes occupied) immediately.

Reporting Interval			
Access	NFC Memory Area	Page	Remarks
R/W	PIN Protected	0x4A	Byte [0:1] TX_INTERVAL_UNOCCUPIED (Default: 0x78 = 120 seconds) Byte [2:3] TX_INTERVAL_OCCUPIED (Default: 0x3C = 60 seconds)

Table 18 – Reporting Interval

7.6.10 Low Power Mode

EMDCB can be configured to be in low power mode where radio transmission is disabled. This is intended mainly to conserve energy during periods of storage and transport.

Low power mode can be entered either by means of pressing the LRN button for 3 seconds as described in chapter 0 or by setting the LOW_POWER_MODE field shown in Table 19 to 0x01.

Likewise, low power mode can be exited either by pressing the LRN shortly as described in chapter 0 or by clearing the LOW_POWER_MODE field shown in Table 19 to 0x00.

Low Power Mode			
Access	NFC Memory Area	Page	Remarks
R/W	PIN Protected	0x4B	Byte [0] LOW_POWER_MODE 0x00 = Normal Operation Mode (Default) 0x01 = Low Power Mode Byte [1:3] RFU

Table 19 – Low Power Mode

8 Regulatory notes

8.1 European Union

8.1.1 Declaration of conformity

Hereby, EnOcean GmbH, declares that this radio equipment is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU. A copy of the Declaration of Conformity can be obtained from the product webpage at www.enocean.com

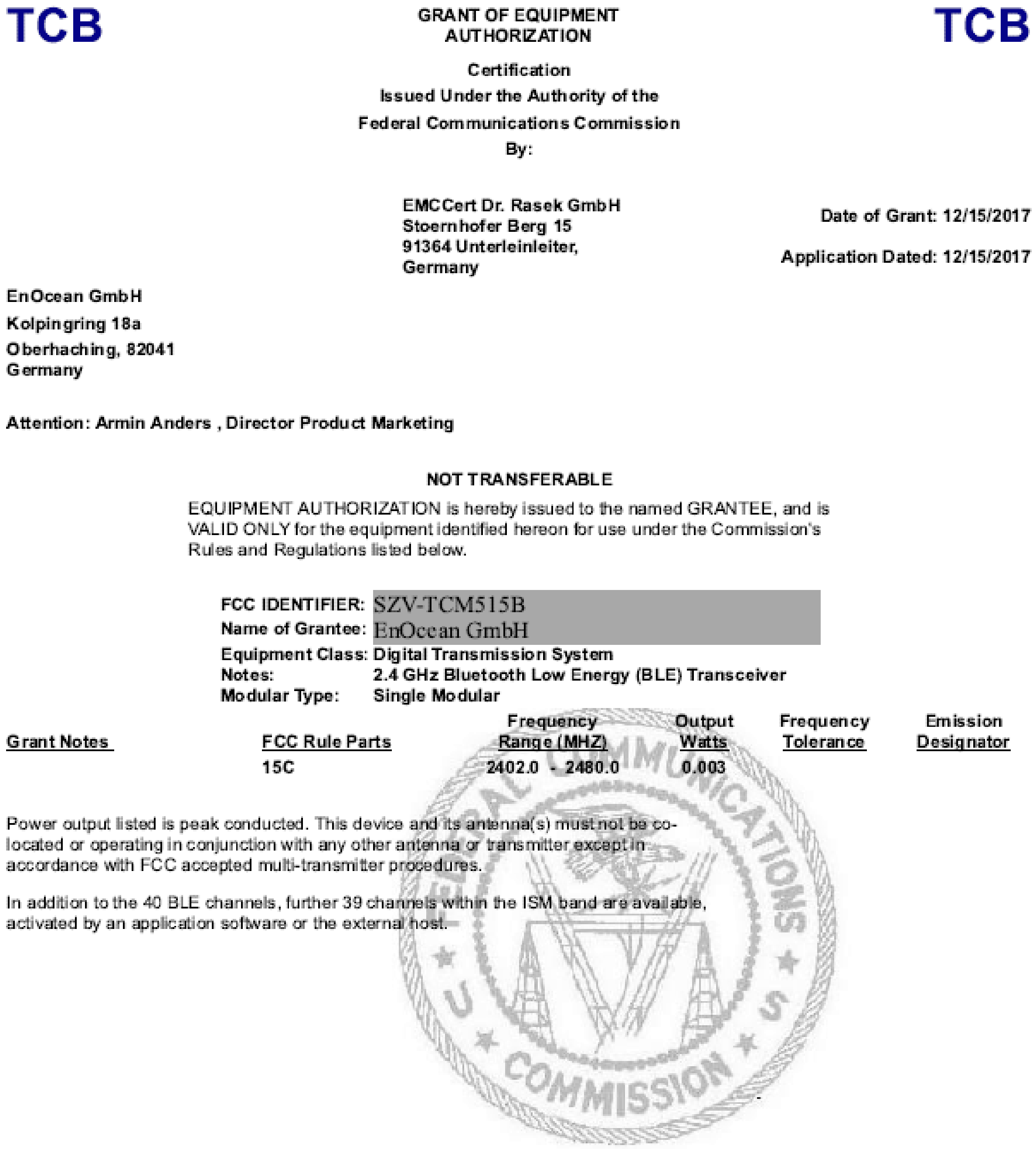
8.1.2 Waste treatment

WEEE Directive Statement of the European Union
The marking below indicates that this product should not be disposed with other household wastes throughout the EU. To prevent possible harm to the environment or human health from uncontrolled waste disposal, recycle it responsibly to promote the sustainable reuse of material resources.
Germany: WEEE-Reg-No.: DE 93770561

BATTERY Directive
This symbol below indicates that batteries must not be disposed of in the domestic waste as they contain substances which can be damaging to the environment and health. Please dispose of batteries in designated collection points.
Germany: UBA Reg-No.: 21008516

8.2 FCC (United States)

8.2.1 FCC (United States) Certificate



TCB

GRANT OF EQUIPMENT
AUTHORIZATION

TCB

Certification
Issued Under the Authority of the
Federal Communications Commission
By:

EMCCert Dr. Rasek GmbH
Stoernhofer Berg 15
91364 Unterleinleiter,
Germany

Date of Grant: 12/15/2017

Application Dated: 12/15/2017

EnOcean GmbH
Kolpingring 18a
Oberhaching, 82041
Germany

Attention: Armin Anders , Director Product Marketing

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and is VALID ONLY for the equipment identified hereon for use under the Commission's Rules and Regulations listed below.

FCC IDENTIFIER:	SZV-TCM515B
Name of Grantee:	EnOcean GmbH
Equipment Class:	Digital Transmission System
Notes:	2.4 GHz Bluetooth Low Energy (BLE) Transceiver
Modular Type:	Single Modular

Grant Notes	FCC Rule Parts	Frequency Range (MHZ)	Output Watts	Frequency Tolerance	Emission Designator
	15C	2402.0 - 2480.0	0.003		

Power output listed is peak conducted. This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC accepted multi-transmitter procedures.

In addition to the 40 BLE channels, further 39 channels within the ISM band are available, activated by an application software or the external host.

8.2.2 FCC (United States) Regulatory Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) this device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

8.2.3 FCC Usage Conditions

TCM 515B is a RF module approved for Single Modular use. It is incorporated into EMDCB as OEM installation using an approved antenna.

The module is optimized to operate using small amounts of energy, and may be powered by a battery. The module transmits short radio packets comprised of control signals, (in some cases the control signal may be accompanied with data) such as those used with alarm systems, door openers, remote switches, and the like.

The module does not support continuous streaming of voice, video, or any other forms of streaming data; it sends only short packets containing control signals and possibly data. The module is designed to comply with, has been tested according to 15.231(a-c), and has been found to comply with each requirement.

Thus, EMDCB containing the TCM 515B radio module can be operated in the United States without additional Part 15 FCC approval (approval(s) for unintentional radiators may be required for the OEM's finished product), under EnOcean's FCC ID number if the OEM requirements are met.

8.2.4 FCC OEM Requirements

In order to use EnOcean’s FCC ID number, the OEM must ensure that the following conditions are met:

- The Original Equipment Manufacturer (OEM) must ensure that FCC labeling requirements are met. This includes a clearly visible label on the outside of the final product. Attaching a label to a removable portion of the final product, such as a battery cover, is not permitted.

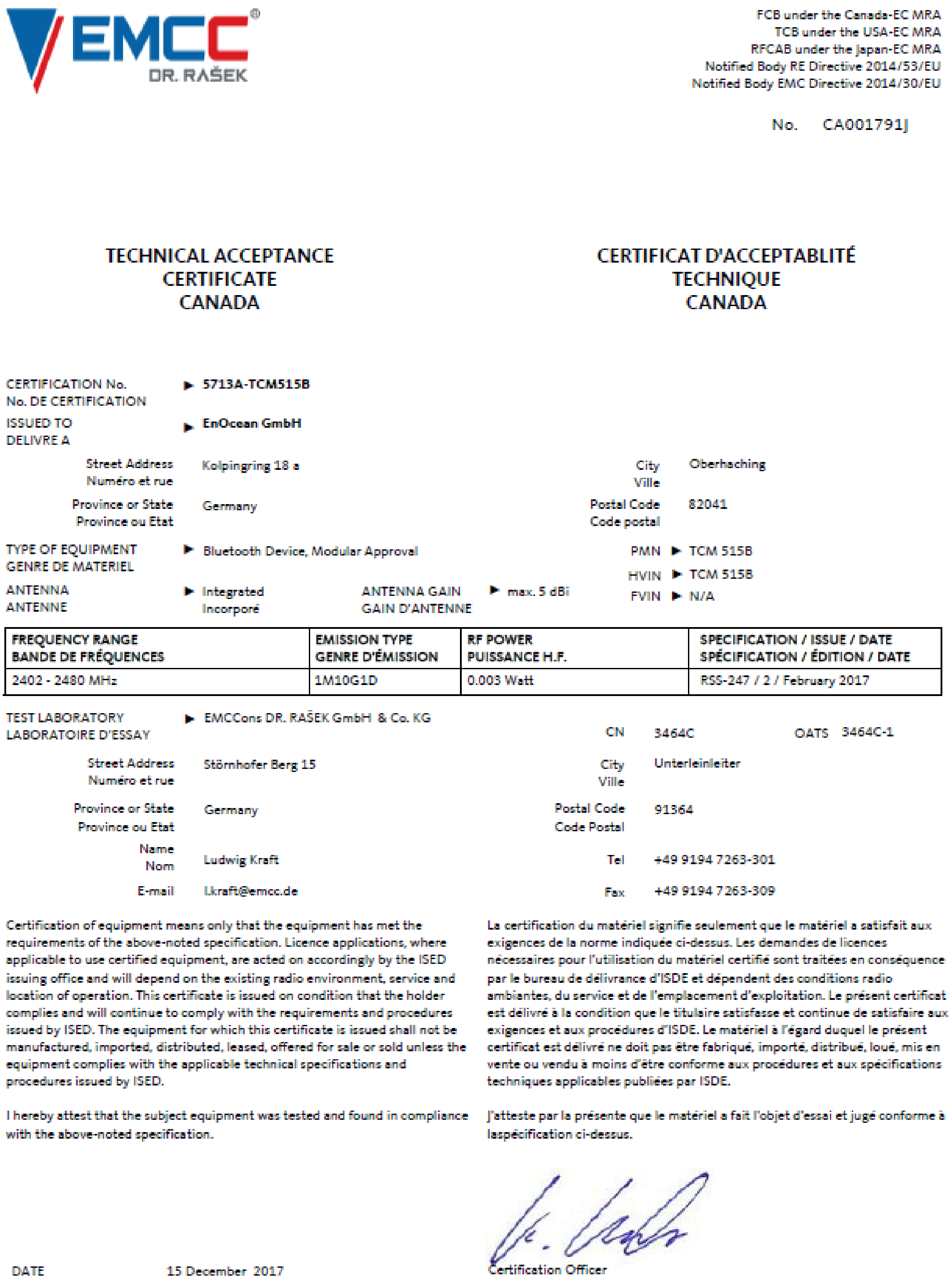
- The label must include the following text:
  Contains FCC ID: SZV-TCM515B
  The enclosed device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (i.) this device may not cause harmful interference and (ii.) this device must accept any interference received, including interference that may cause undesired operation.

- The FCC identifier or the unique identifier, as appropriate, must be displayed on the device.

- The user manual for the end product must also contain the text given above.

8.3 ISED (Industry Canada)

8.3.1 ISED (Industry Canada) Certificate



EMCC® DR. RAŠEK

FCB under the Canada-EC MRA
TCB under the USA-EC MRA
RFCAB under the Japan-EC MRA
Notified Body RE Directive 2014/53/EU
Notified Body EMC Directive 2014/30/EU

No. CA001791J

TECHNICAL ACCEPTANCE
CERTIFICATE
CANADA

CERTIFICAT D'ACCEPTABLITÉ
TECHNIQUE
CANADA

CERTIFICATION No. / No. DE CERTIFICATION ▶ **5713A-TCM515B**

ISSUED TO / DELIVRE A ▶ **EnOcean GmbH**

Street Address / Numéro et rue: Kolpingring 18 a
City / Ville: Oberhaching

Province or State / Province ou Etat: Germany
Postal Code / Code postal: 82041

TYPE OF EQUIPMENT / GENRE DE MATERIEL ▶ Bluetooth Device, Modular Approval
PMN ▶ TCM 515B
HVIN ▶ TCM 515B

ANTENNA / ANTENNE ▶ Integrated / Incorporé
ANTENNA GAIN / GAIN D'ANTENNE ▶ max. 5 dBi
FVIN ▶ N/A

FREQUENCY RANGE BANDE DE FRÉQUENCES	EMISSION TYPE GENRE D'ÉMISSION	RF POWER PUISSANCE H.F.	SPECIFICATION / ISSUE / DATE SPÉCIFICATION / ÉDITION / DATE
2402 - 2480 MHz	1M10G1D	0.003 Watt	RSS-247 / 2 / February 2017

TEST LABORATORY / LABORATOIRE D'ESSAY ▶ EMCCons DR. RAŠEK GmbH & Co. KG
CN 3464C
OATS 3464C-1

Street Address / Numéro et rue: Störnhofer Berg 15
City / Ville: Unterleinleiter

Province or State / Province ou Etat: Germany
Postal Code / Code Postal: 91364

Name / Nom: Ludwig Kraft
Tel: +49 9194 7263-301

E-mail: l.kraft@emcc.de
Fax: +49 9194 7263-309

Certification of equipment means only that the equipment has met the requirements of the above-noted specification. Licence applications, where applicable to use certified equipment, are acted on accordingly by the ISED issuing office and will depend on the existing radio environment, service and location of operation. This certificate is issued on condition that the holder complies and will continue to comply with the requirements and procedures issued by ISED. The equipment for which this certificate is issued shall not be manufactured, imported, distributed, leased, offered for sale or sold unless the equipment complies with the applicable technical specifications and procedures issued by ISED.

I hereby attest that the subject equipment was tested and found in compliance with the above-noted specification.

La certification du matériel signifie seulement que le matériel a satisfait aux exigences de la norme indiquée ci-dessus. Les demandes de licences nécessaires pour l'utilisation du matériel certifié sont traitées en conséquence par le bureau de délivrance d'ISDE et dépendent des conditions radio ambiantes, du service et de l'emplacement d'exploitation. Le présent certificat est délivré à la condition que le titulaire satisfasse et continue de satisfaire aux exigences et aux procédures d'ISDE. Le matériel à l'égard duquel le présent certificat est délivré ne doit pas être fabriqué, importé, distribué, loué, mis en vente ou vendu à moins d'être conforme aux procédures et aux spécifications techniques applicables publiées par ISDE.

J'atteste par la présente que le matériel a fait l'objet d'essai et jugé conforme à laspécification ci-dessus.

DATE 15 December 2017

Certification Officer

8.3.2 ISED (Industry Canada) Regulatory Statement

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

(1) this device may not cause interference, and

(2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.”

9 Product history

Table 20 below lists the product history of EMDCB.

Revision	Release date	Key changes versus previous revision
CA-01	December 2018	First release for lead customers
CA-02	June 2019	Addition of 2 Mbit mode

Table 20 – Product History

A Parsing EMDCB telegrams

This chapter provides examples of EMDCB telegrams and shows how to interpret them.

A.1 Data telegram example

We consider the following raw data (excluding CRC) captured from an EMDCB device:

```
D6 BE 89 8E 42 1C C4 00 00 00 00 E5 15 FF DA 03 57 E2 01 00 02 AA 44 D6 00 45 35 00
20 02 C8 CC 57 12
```

A.1.1 BLE advertising frame structure

The message above can be parsed according to the Bluetooth standard for advertising messages as shown in Table 21 below.

Field	Length	Data	Interpretation
BLE Access Address	4 byte	0x8E89BED6	Constant (always used)
BLE Frame Control	2 byte	0x1C42	Length = 28 byte
BLE Source Address	6 byte	0xE500000000C4	Device-unique address
Length of payload	1 byte	0x15	21 byte of payload follow
Type of payload	1 byte	0xFF	Manufacturer-specific data
Manufacturer ID	2 byte	0x03DA	EnOcean GmbH
Payload	18 byte	57 E2 01 00 02 AA 44 D6 00 45 35 00 20 02 C8 CC 57 12	

Table 21 – Advertising message parsing

A.1.2 Data telegram payload

The EnOcean payload can be parsed as shown in Table 22 below.

Field	Length	Data	Interpretation
Sequence Counter	4 byte	0x0001E257	Incrementing message counter
Sensor Data	10 byte	02 AA 44 D6 00 45 35 00 20 02	
Telegram Signature	4 byte	0xC8CC5712	Authentication signature

Table 22 – EnOcean data telegram payload parsing

A.1.3 Sensor data

The sensor data can be parsed as shown in Table 23 below.

Descriptor	Data Length	Type	Data	Value
0x02	0b00 (8 bit)	0b000010 (Energy Level)	0xAA	85 %
0x44	0b01 (16 bit)	0b000100 (Solar Cell Illuminance)	0x00D6	214 lx
0x45	0b01 (16 bit)	0b000101 (Sensor Illuminance)	0x0035	53 lx
0x20	0b00	0b100000 (Occupancy)	0x02	Occupied

Table 23 – Sensor data parsing

A.2 Commissioning telegram example

We consider the following advertising data (excluding CRC) captured from the same EMDCB device as in the previous chapter:

```
D6 BE 89 8E 42 25 C4 00 00 00 00 E5 1E FF DA 03 56 E2 01 00 3E 9E 0D E9 C2 53 86 B6
C4 F0 70 64 2E 19 E0 36 80 C4 00 00 00 00 E5
```

A.2.1 BLE advertising data

The advertising data given above can be parsed according to the Bluetooth standard for advertising frames as shown in Table 24 below.

Field	Length	Data	Interpretation
BLE Access Address	4 byte	`0x8E89BED6`	Constant (always used)
BLE Frame Control	2 byte	`0x2542`	Length = 37 byte
BLE Source Address	6 byte	`0xE500000000C4`	Device-unique address
Length of payload	1 byte	`0x1E`	30 byte of payload follow
Type of payload	1 byte	`0xFF`	Manufacturer-specific data
Manufacturer ID	2 byte	`0x03DA`	EnOcean GmbH
Payload	27 byte	`56 E2 01 00 3E 9E 0D E9 C2 53 86 B6 C4 F0 70 64 2E 19 E0 36 80 C4 00 00 00 00 E5`	

Table 24 – Advertising data parsing

A.2.2 Commissioning telegram payload

The payload of the commissioning telegram can be parsed as shown in Table 25 below.

Field	Length	Data	Interpretation
Sequence Counter	4 byte	`0001E256`	Incrementing message counter
Field Identfier	1 byte	`0x3E`	Commissioning Telegram (22 byte)
Device Key	16 byte	`9E0DE9C25386B6C4F070642E19E03680`	
Source Address	6 byte	`0xE500000000C4`	

Table 25 – Commissioning telegram payload parsing

B Authentication example for EMDCB telegrams

We consider the data telegram discussed in chapter A.1 and assume this shall be authenticated by means of a security key known to both the sender and the receiver.

The security key could be obtained in the following way:

- From the commissioning telegram as specified in chapter A.2
- From the device label as specified in chapter 6.2
- From the NFC configuration memory as described in chapter 7

B.1 Input data

The purpose of the security processing is to calculate a unique signature that can be used to verify authenticity (telegram has not been modified) and originality (telegram comes from the assumed sender) of a telegram.

The input data for the authentication process is listed in Table 26 below.

Parameter	Comment / Description	Example
Source Address	Unique source address of the sensor module (little endian)	C400000000E5 (little endian representation of 0xE500000000C4)
Input Data	Telegram data to be authenticated	15 FF DA 03 57 E2 01 00 02 AA 44 D6 00 45 35 00 20 02
Input Length	Length of input data (in bytes, encoded using 2 bytes)	0x0015 (21 byte)
Sequence Counter	Incrementing counter to avoid replay Part of the input data (byte 4 … 7)	57E20100 (little endian representation of 0x0001E257)
Security Key	128 bit random key that is known both to sender and receiver	9E0DE9C25386B6C4F070642E19E03680
Signature from Sender	32 Bit signature that will be checked using the security key	C8CC5712

Table 26 – Input data

B.2 Constant algorithm parameters

The RFC3610 implementation requires two constant algorithm parameters:

- Length field size (in byte)
  This is the size of the field used to encode the length of the input data (which is the payload to be authenticated).
  The maximum size of sensor payload to be authenticated is 31 byte; therefore one byte would be easily sufficient to encode the payload size. The minimum value permitted by the standard is however 2 bytes which is therefore chosen.

- Signature size (in byte)
  The desired signature size is 4 byte for sensor data telegrams

Table 27 below summarizes these algorithm parameters.

Parameter	Comment / Description	Example
Length Field Size	Size (in bytes) of the field used to encode the input length	2 (always, minimum permissible size)
Signature Size	Desired size (in byte) of the signature generated by the algorithm	4 (always)

Table 27 – Constant algorithm parameters

The RFC3610 implementation derives two algorithm parameters – M’ and L’ – based on the constant algorithm parameters and uses them to construct A0_Flag and B_0_Flag which – together with the iteration counter i – are required for subsequent processing.

The value of these internal parameters - listed in Table 28 below - is the same for all EnOcean BLE telegrams.

Parameter	Comment / Description	Example
M’	Binary encoded output length `M’ = (Output length / 2) - 1`	`0b001` (always)
L’	Binary encoded length field size `L’ = length field size - 1`	`0b001` (always)
A0_Flag	`L’`	`0x01` (always)
B0_Flag	`(0b01<<6) + (M’<<3) + L’`	`0x49` (always)
I	Iteration counter	`0x0000 (always)`

Table 28 – Constant internal parameters

B.3 Intermediate parameters

The RFC3610 implementation used in EnOcean BLE products derives four internal parameters – Nonce, A0, B0, B1 and B2 – based on the telegram specific input data and the constant internal parameters.

These variable internal parameters are described in Table 29 below. The values of these parameters are calculated based on the input data given in chapter B.1.

Parameter	Comment / Description	Value in the example
Nonce	13 byte initialization vector based on concatenation of 6 byte source address, 4 byte sequence counter and 3 byte 0x00 padding	C400000000E557E20100000000
A0	A0_Flag followed by Nonce followed by 2 byte 0x00	01C400000000E557E201000000000000
B0	B0_Flag followed by Nonce followed by 2 byte 0x00 (no message to encode)	49C400000000E557E201000000000000
B1	Input Length followed by first 14 byte of Input Data	001515FFDA0357E2010002AA44D60045
B2	Remaining Input Data (up to 16 byte) with 0x00 padding to reach 16 byte in total	35002002000000000000000000000000

Table 29 – Intermediate parameters

B.4 RFC3610 execution sequence

The RFC3610 algorithm uses the variable internal parameters A_0, B_0, B_1 and B_2 together with the private key to generate the authentication vector T_0 using four AES-128 and three XOR operations. The algorithm execution sequence is shown in Figure 37 below.

The first four bytes of T_0 are then used to authenticate EnOcean BLE multi-sensor data telegrams.

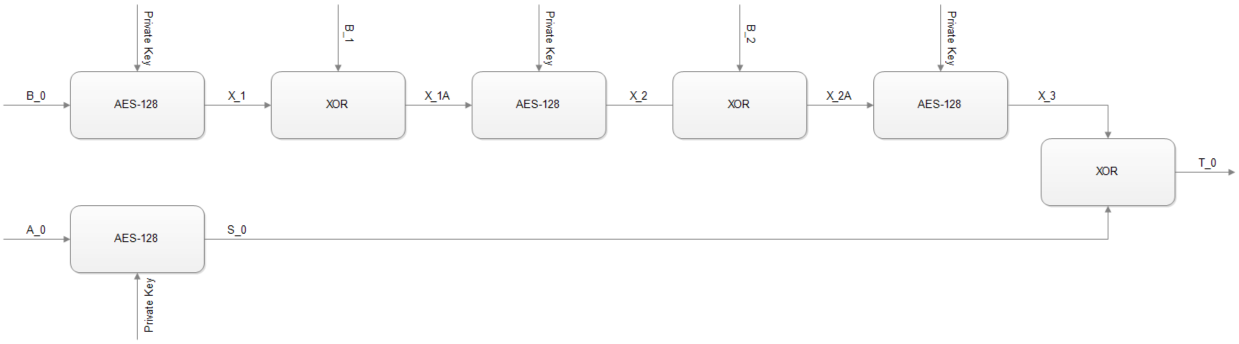


Figure 37 – RFC3610 execution sequence

B.5 Execution example

At the time of writing, a suitable online AES calculator could be found here:
http://testprotect.com/appendix/AEScalc

Likewise, a suitable online XOR calculator could be found here:
http://xor.pw/?

We can now calculate the signature using a sequence of AES128 and XOR operations as shown in Figure 37 as follows:

```
X_1 = AES128(B0, Key)
X_1 = AES128(49C400000000E557E201000000000000, 9E0DE9C25386B6C4F070642E19E03680)
X_1 = 97F967605F8B20A988A026AC76B0E4E0

X_1A = XOR(X_1, B_1)
X_1A = XOR(97F967605F8B20A988A026AC76B0E4E0, 001215FFDA0357E2010002AA44D60045)
X_1A = 97EB729F8588774B89A024063266E4A5

X_2 = AES128(X_1A, Key)
X_2 = AES128(97EB729F8588774B89A024063266E4A5, 9E0DE9C25386B6C4F070642E19E03680)
X_2 = 8CD6013AFFB05E19DA7891398FFA00B4

X_2A = XOR(X_2, B_2)
X_2A = XOR(8CD6013AFFB05E19DA7891398FFA00B4, 35002002000000000000000000000000)
X_2A = B9D62138FFB05E19DA7891398FFA00B4

X_3 = AES128(X_2A, Key)
X_3 = AES128(B9D62138FFB05E19DA7891398FFA00B4,9E0DE9C25386B6C4F070642E19E03680)
X_3 = 1FA1970E831CFA1C445EC14639CB4AFE


S_0 = AES128(A0, Key)
S_0 = AES128(01C400000000E557E201000000000000,9E0DE9C25386B6C4F070642E19E03680)
S_0 = D76DC01C1302BEC9C7DC61042CE71D2C

T_0 = XOR(X_3, S_0)
T_0 = XOR(1FA1970E831CFA1C445EC14639CB4AFE, D76DC01C1302BEC9C7DC61042CE71D2C)
T_0 = C8CC5712901E44D58382A042152C57D2
```

The calculated signature is formed by the first four bytes of `T_0`, i.e. it is `C8CC5712`.

The calculated signature matches the signature that was transmitted as part of the data telegram payload (see chapter A.1).

This proves that the telegram originates from a sender that possesses the same security key and the telegram content has not been modified.

C Address resolution for resolvable private addresses (RPA)

EMDCB provides the option to obfuscate its identity by means of using resolvable private addresses (RPA) as described in chapter 4.4.2. The following chapters describe how to resolve such addresses.

C.1 RPA resolution flow

The execution flow for resolving private addresses (RPA) is shown in Figure 38 below.

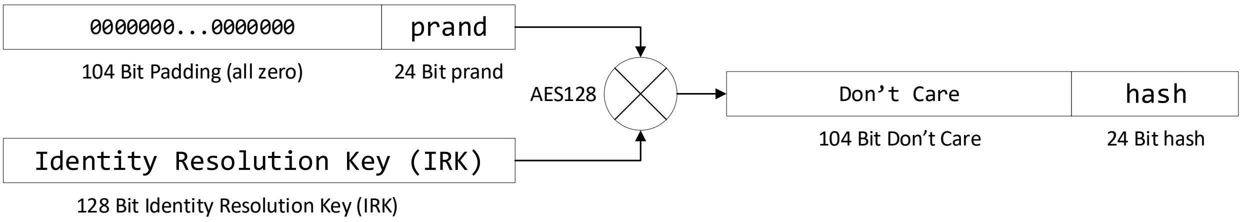

0000000...0000000
prand
104 Bit Padding (all zero)
24 Bit prand
AES128
Don't Care
hash
104 Bit Don't Care
24 Bit hash
Identity Resolution Key (IRK)
128 Bit Identity Resolution Key (IRK)

Figure 38 – Execution flow for resolving private addresses (RPA resolution)

The input to the RPA resolution flow are the `prand` part of the resolvable private address field of the received telegram together with one (or several) locally stored IRK.

The receiver will then try for each locally stored IRK if the `hash` generated using the execution flow above matches the `hash` part of the resolvable private address field of the received telegram. If it does then the IRK identifies the device from which this telegram originated.

C.2 Obtaining the IRK

EMDCB uses its device-unique random private security key as IRK. This key is programmed at manufacturing and can be changed via the NFC interface as described in chapter 7.6.6.

The IRK could be obtained in the following way:

- From the commissioning telegram as specified in chapter A.2
- From the NFC configuration memory as described in chapter 7
- From the device label as specified in chapter 6.2 (if the factory-programmed security key has not been changed via the NFC Interface)

C.3 Address resolution example

We consider an EMDCB device with the following IRK:

```
BE759A027A4870FD242794F4C45220FB
```

We further consider a telegram having the following resolvable private address:

```
493970E51944
```

We will now test if this resolvable private address was generated using the IRK above.

Referring to the resolvable private address structure shown in Figure 15, we split the resolvable private address into `prand` and `hash` as follows:

```
prand  = (RPA && 0xFFFFFF000000) >> 24
prand  = 0x493970

hash   = RPA && 0x000000FFFFFF
hash   = 0xE51944
```

Next, we verify the address mode by looking at the two most significant bit of `prand`:

```
mode   = (prand && 0xC00000) >> 22
mode   = 0b01
```

Referring to chapter 4.4.2, the setting of `0b01` indicates resolvable private address mode.

To generate the hash, we add 104 bit of padding (all zeros) to `prand`:

```
0x00000000000000000000000000493970
```

We can now generate the hash as AES128 operation between the IRK and the thus padded `prand`:

```
hash   = AES128(IRK; Padded prand)
hash   = AES128(0xBE759A027A4870FD242794F4C45220FB;
               0x00000000000000000000000000493970)
```

At the time of writing, a suitable online AES calculator could be found here:
http://testprotect.com/appendix/AEScalc

With this, we can calculate the result as:

```
hash   = 0x286ACB1F9C8A80EE21B3F02225E51944
```

Using this result, we can verify that the lowest 24 bit of the calculated `hash` (`0xE51944`) match the `hash` that was received as part of the resolvable private address. Therefore the transmitter of this telegram used this specific IRK to generate this resolvable private address.