EASYFIT by EnOcean

EMDCB BLUETOOTH LOW ENERGY MOTION DETECTOR AND LIGHT LEVEL SENSOR

EMDCB

Bluetooth Low Energy Motion Detector And Light Level 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
1.4	MKA	MKA	24.03.2020	Update for DA-04 product revision Improved description of NFC interface Improved document structure

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 with 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. 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 ambient light is not sufficiently available, EMDCB provides the option to use 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 Can be reduced to 0 dBm 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	1 Mbit/s GFSK (default setting) 2 Mbit/s GFSK (selectable via NFC)
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) Consistent low light (65 lux for 5 hrs every day) Total Darkness	 20 years 15 years 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 harvesting available light from the environment.

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. Configuration of EMDCx parameters is possible via an integrated NFC (ISO 14443) interface.

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 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. The internal NFC antenna (not visible from the outside) provides access to the NFC configuration interface.

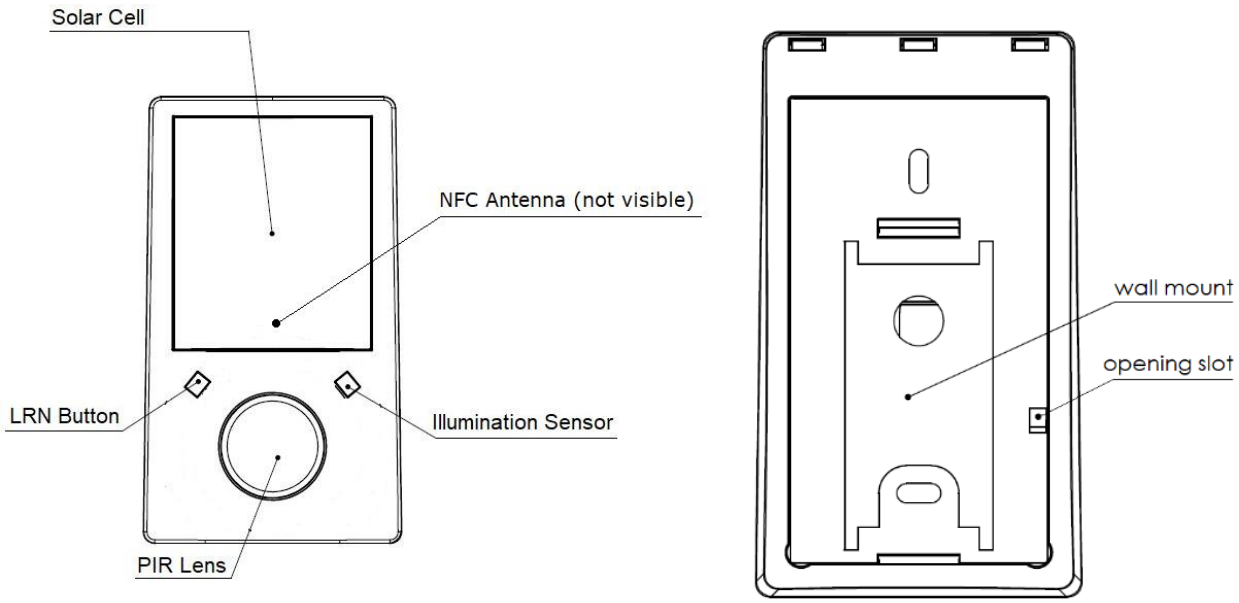

Figure 2 – EMDCB front and rear view

2.4 Internal product interface

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

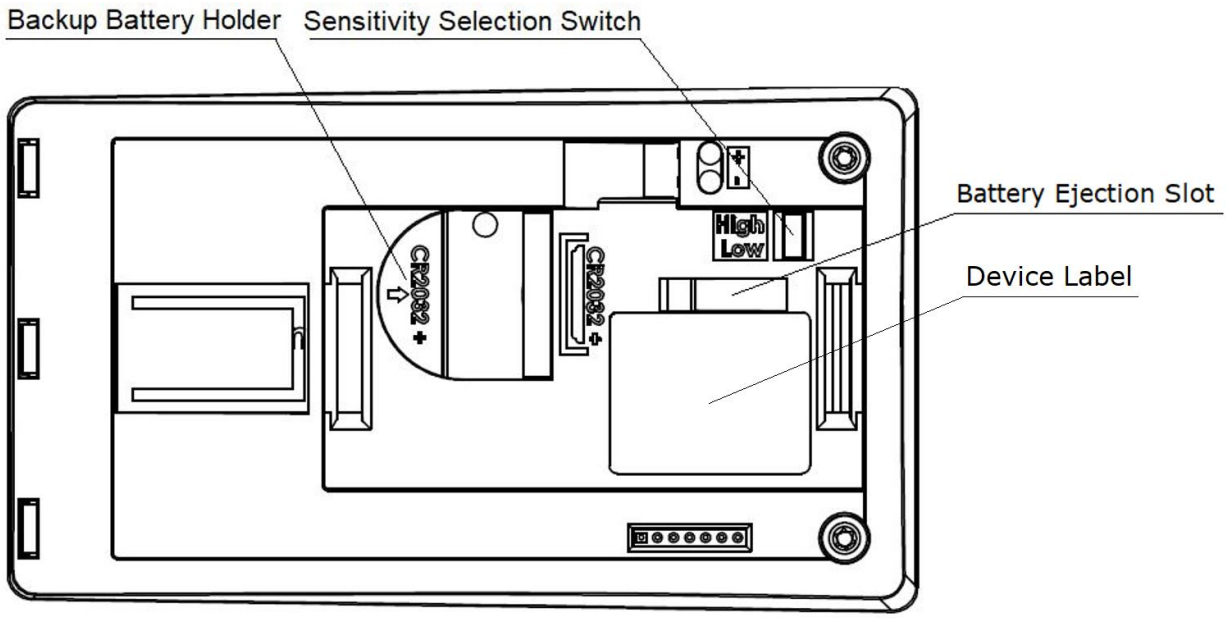

Figure 3 – EMDCB internal view

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 screwdriver (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.

2.5 Functional modes

EMDCB supports three types of functional modes:

- Standard operation mode
- Walk test mode
- Standby (sleep) mode

These modes are described below.

2.5.1 Standard operation mode

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 3.1, the light level sensing functionality in chapter 3.2 and the data telegram transmission and format in chapters 4 and 6 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 reporting intervals under specific conditions as described in chapter 2.6. In case of reducing the reporting interval, the resulting increase in required energy (provided by the available light or a backup battery) must be considered.

2.5.2 Walk test mode

Walk test mode is used to verify the motion detection coverage of the device via visual feedback from the LED which will blink whenever motion is detected. Walk test mode can be selected using the LRN button as described in chapter 4.1 and will be active for a period of 120 seconds.

2.5.3 Standby (Sleep) mode

Standby (Sleep) mode is used to conserve as much energy as possible during periods of storage or transport. All functionality – except those needed to return to standard operation mode – are disabled in this mode. Standby mode can be selected using the LRN button as described in chapter 4.1 or using the NFC interface as described in chapter 10.5.17.

2.6 Reporting interval

The reporting interval of EMDCB defines the interval between two status updates, i.e. between two data telegrams.

EMDCB allows using different reporting intervals for occupied status (motion is detected) and for unoccupied status (no motion is detected). Additionally, it is possible to define lower reporting intervals for the case that a certain light level is exceeded so that EMDCB reports more often for instance if a room is brightly lit.

The minimum possible reporting interval is 3 seconds and the maximum possible transmission interval is 65535 seconds. Please note that lowering the reporting intervals will increase power consumption. Therefore, the default settings should only be lowered if sufficient ambient light is available.

EMDCB will immediately report an initial motion detection after a period without detected motion independent of the selected configuration.

2.6.1 Unoccupied reporting interval

The unoccupied reporting interval determines the interval between two status updates of EMDCB while no motion is detected.

The default setting for the unoccupied reporting interval is one status update every 120 seconds (2 minutes). This interval can be adjusted using the UNOCCUPIED_TX_INTERVAL NFC register as described in chapter 10.5.18.

Figure 4 below illustrates the use of the unoccupied reporting interval.

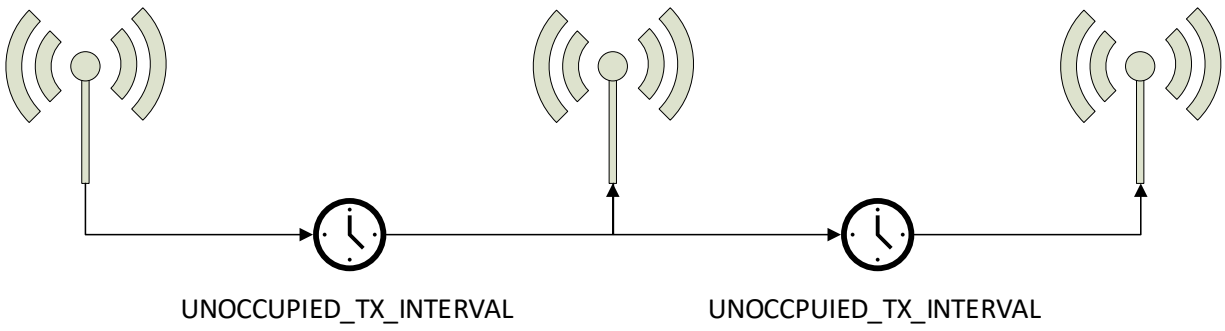

Figure 4 – Unoccupied reporting interval

2.6.2 Occupied reporting interval

If a room is occupied, then it might be desirable to receive status updates more often for instance to report the current light level. EMDCB is therefore by default configured to use a lower reporting interval, i.e. a higher update rate, while a room is occupied (i.e. while motion is detected).

The default setting of the occupied reporting interval is 60 seconds. This setting can be changed using the OCCUPIED_TX_INTERVAL NFC register as described in chapter 10.5.19.

Figure 5 below illustrates the use of the occupancy-controlled reporting interval.

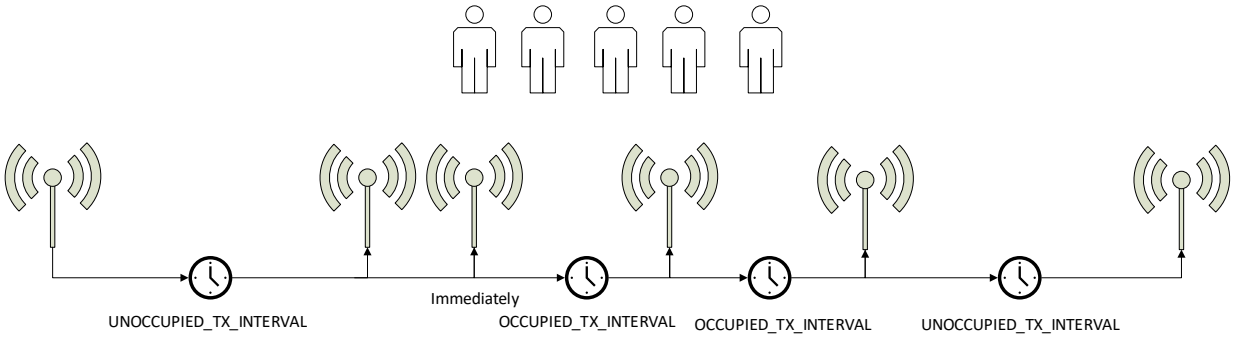

Figure 5 – Occupied versus unoccupied reporting interval

2.6.3 Illumination-controlled reporting interval

If sufficient ambient light is available, then it might be desirable to receive status updates more often. For this, there are typically two main use cases:

- Adjust the update rate based on the ambient light available for harvesting
- Report more often during daytime (or when an office is lit) and less often during night-time (or when an office is dark) to adapt the reporting to the usage pattern

In both cases, the lower update rate (defined by the standard reporting interval) would be used whenever the ambient light level is below a certain threshold. The higher update rate (defined by the light level-controlled reporting interval) would be used whenever the ambient light level is above a certain threshold.

This feature is available in EMDCB starting with product revision DA-04 onwards (devices produced in model year 2020 or later).

In these devices, the light threshold and the reporting interval rate to be used when the measured light level is above the threshold can be configured using the NFC interface as defined in chapter 10.5.20. Previous revisions (before DA-04) will ignore this setting.

It is possible to define different thresholds and reporting intervals for the solar cell (harvested energy) and the light level sensor (measured light level).

Figure 6 below illustrated the use of the illumination-controlled reporting interval.

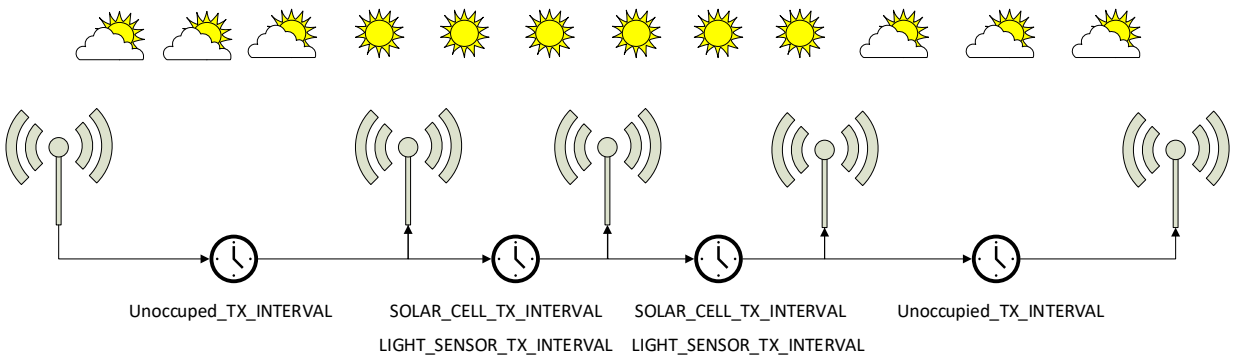

Figure 6 – Illumination-controlled reporting interval

2.6.4 Arbitration between reporting intervals

If more than one condition for a lower reporting interval applies – e.g. if a room is both occupied and brightly lit – then the lowest of the corresponding reporting intervals will be selected.

3 Sensor functionality

EMDCB implements the following sensor functions:

- Motion detection using the passive infrared sensor (PIR)
- Illumination measurement using the light level sensor
- Illumination measurement using the solar cell
- Energy level of the energy store
- Supply voltage of the backup battery (if present)

These functions are described in detail in the subsequent chapters.

3.1 Motion detection

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

3.1.1 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 7 below shows the PIR detection pattern.

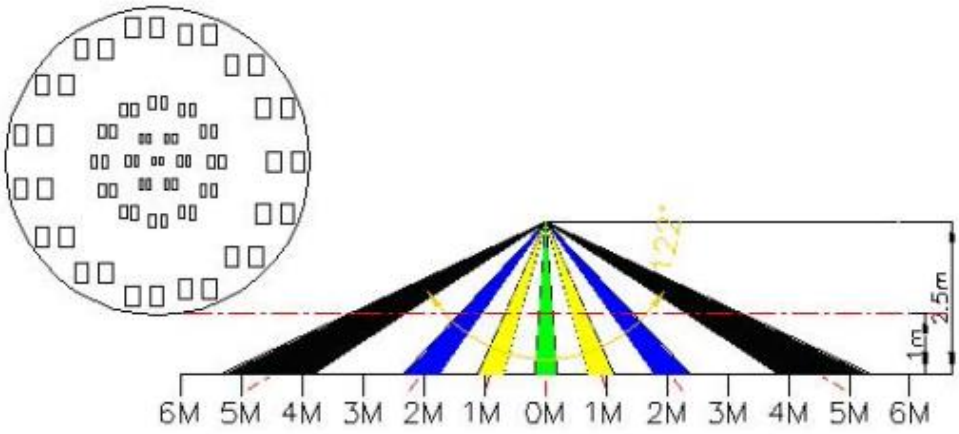

Figure 7 – EMDCB PIR detection pattern

3.2 Illumination measurement (light level sensor)

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

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

Figure 8 shows the spectrum response of the EMDCB illumination sensor compared to that of the human eye.

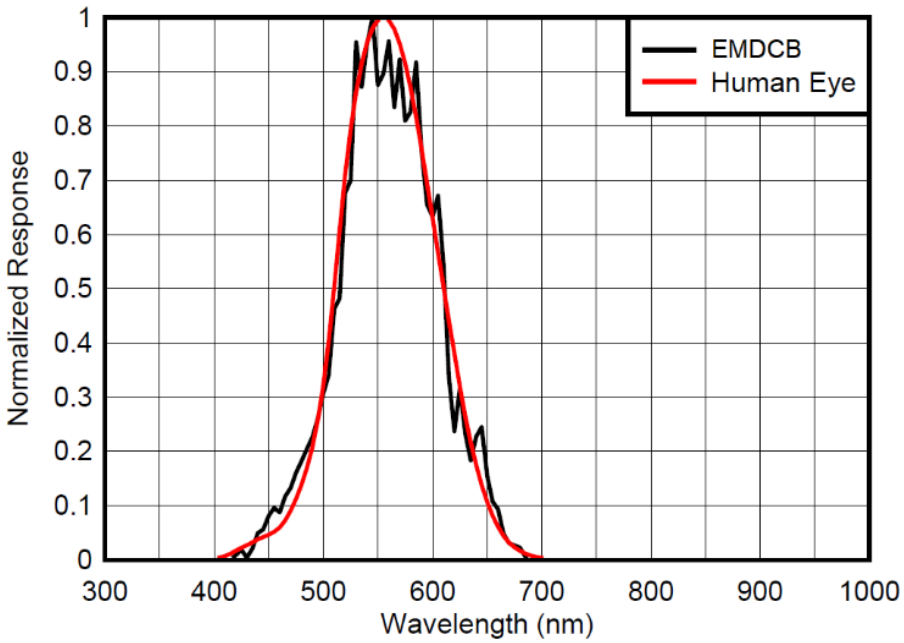

Figure 8 – Spectrum response of the illumination sensor

3.3 Illumination measurement (solar cell)

EMDCB can report the light level by measuring the energy generated by the solar cell.

This functionality can be used both to ensure that 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 10.5.15. By default, the reporting is disabled.

3.4 Energy level

EMDCB can measure the voltage of the internal energy store which stores the harvested energy to supply the device when the ambient light is insufficient to power the device.

Based on the measured voltage, EMDCB will estimate the energy level (amount of remaining energy) and report this as a percentage between 0% (empty) and 100% (fully charged).

Reporting of the energy level can be enabled and disabled via the NFC interface as described in chapter 10.5.15.

By default, the reporting of the remaining energy is enabled if no backup battery is present. If a backup battery is present, then by default its supply voltage is reported instead.

Note that the reported energy level can only provide rough guidance as the actual energy level depends on several factors (most notably the ambient temperature).

3.5 Backup battery voltage

EMDCB can measure the supply voltage level of external backup battery used to supply the device when the available ambient light is insufficient for energy harvesting operation.

Reporting of the backup battery voltage can be enabled and disabled via the NFC interface as described in chapter 10.5.15.

By default, the backup battery voltage is reported if a backup battery is present. Otherwise the energy level of the internal energy store is reported instead.

4 User interface

The user interface of EMDCB consist of the following items:

- LRN button and LED
- Sensitivity selection switch
- Backup battery interface

Please refer to chapters 2.3 and 2.4 to identify the location of these items.

4.1 LED

EMDCB contains an indication LED used to provide user feedback. By default, the LED will blink shortly whenever a telegram indicating occupied (motion detected) status is sent. This indication can be disabled using the LED_MODE register of the NFC interface as described in chapter 10.5.16. In addition to that, the LED provides a response to LRN button inputs as described below.

4.2 LRN button

Most EMDCB device parameters can be configured using the NFC interface as described in chapter 9. Some of the most common parameters or states can additionally be configured using the LRN button with the LED providing visual feedback. Table 1 below lists those configuration actions.

Type	Timing	EMDCB Response	LED Response
Single Short	< 1s Press	Exit from Sleep Mode Send Learn Telegram	1 short blink
Double Short	< 1s Press, < 1s Release, < 1s Press	Start Walk Test (End after 2 min or upon any button press)	1 short blink every time movement is detected
Triple Short	< 1s Press, < 1s Release, < 1s Press, < 1s Release, < 1s Press	Toggle LED indication	LED enabled: 2 short blinks LED disabled: No feedback
Long	3s < Press < 5s	Enter Sleep Mode (Disable LED and Radio)	Error: No feedback Success: 3 short blinks
Very Long	> 8s Press	Factory Reset	Error: No feedback Success: 3 short blinks

Table 1 – EMDCB LRN button actions

4.3 Factory reset

The EMDCB configuration can be reset to the factory default values by means of a factory reset. Factory reset is triggered by pressing and holding the LRN button for more than 8 seconds as described above.

4.4 Sensitivity selection switch

The sensitivity selection switch allows reducing the detection range from its default radius of up to 5 m to a reduced radius of up to 3 m.

Note that the exact detection radius depends on a number of factors including the mounting height and the ambient temperature.

4.5 Backup battery interface

The backup batter interface allows supplying EMDCB by means of a CR2032 battery in case the available ambient light is insufficient for energy harvesting operation. EnOcean recommends using Renata batteries due to their low self-discharge characteristics.

The CR2032 backup battery can be inserted by gently pushing it into the backup battery slot. Note that the positive terminal (+) must face upwards (away from the PCB). The backup battery can be removed by inserting a screwdriver into the battery ejection slot shown in Figure 3.

5 Radio transmission

5.1 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 10.5.5 and 10.5.6.

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

5.2 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 9 below.

The default interval setting is 20 ms; an alternative setting of 10 ms can be configured via NFC as described in chapter 10.5.8.

Figure 9 – Default radio transmission sequence

5.3 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 5.2 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_CFG` register of the NFC configuration interface as described in chapter 10.5.6.

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 three radio channels to be used. The three-channel sequence is described in chapter 5.3.1 below.
- Two-channel sequence
  In this sequence the radio telegram is transmitted using six transmissions on two radio channels. It is described in chapter 5.3.2 below.
- One-channel sequence
  In this sequence the radio telegram is transmitted using nine transmissions on one radio channel. It is described in chapter 5.3.3 below.

5.3.1 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 CH_REG1, CH_REG2 and CH_REG3 as described in chapter 10.5.5.

In this mode, the telegram will be transmitted on the radio channel selected by CH_REG1 first, immediately followed by a transmission on the radio channel selected by CH_REG2 and a transmission on the radio channel selected by CH_REG3.

The telegram will be transmitted using this sequence three times in total as shown in Figure 10 below.

This transmission uses a default INTERVAL setting of 20 ms; an alternative setting of 10 ms can be configured via NFC as described in chapter 10.5.8.

Figure 10 – Three-channel radio transmission sequence

5.3.2 Two-channel sequence

The two-channel radio transmission sequence transmits radio telegrams on two user-defined radio channels (selected by CH_REG1 and CH_REG2 as described in chapter 10.5.5.) six times in total.

The telegram will in this mode be transmitted on the radio channel selected by CH_REG1 first, immediately followed by a transmission on the radio channel selected by CH_REG2. This is shown in Figure 11 below.

This transmission sequence uses a default INTERVAL setting of 20 ms; an alternative setting of 10 ms can be configured via NFC as described in chapter 10.5.8.

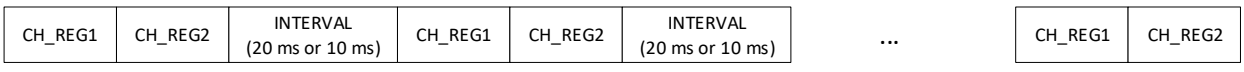

Figure 11 – Two channel radio transmission sequence

5.3.3 One-channel sequence

The one-channel radio transmission sequence transmits radio telegrams on one user-defined radio channel (selected by CH_REG1 as described in chapter 10.5.5.) nine times in total. This is shown in Figure 12 below.

This transmission sequence uses a default INTERVAL setting of 20 ms; an alternative setting of 10 ms can be configured via NFC as described in chapter 10.5.8.

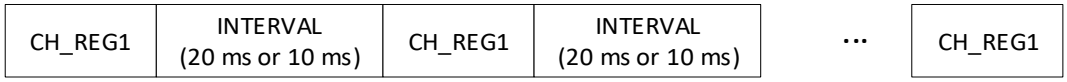

Figure 12 – Single channel radio transmission sequence

6 Telegram format

EMDCB transmits Bluetooth Low Energy (BLE) advertising telegrams in the 2.4 GHz band.

For detailed information about the Bluetooth Low Energy standard in general and Bluetooth Advertising in particular, please refer to the applicable specifications.

Figure 13 below summarizes the BLE advertising frame structure.

Figure 13 – BLE frame structure

Figure 14 below shows specific properties used by EMDCB within the general BLE advertising frame structure.

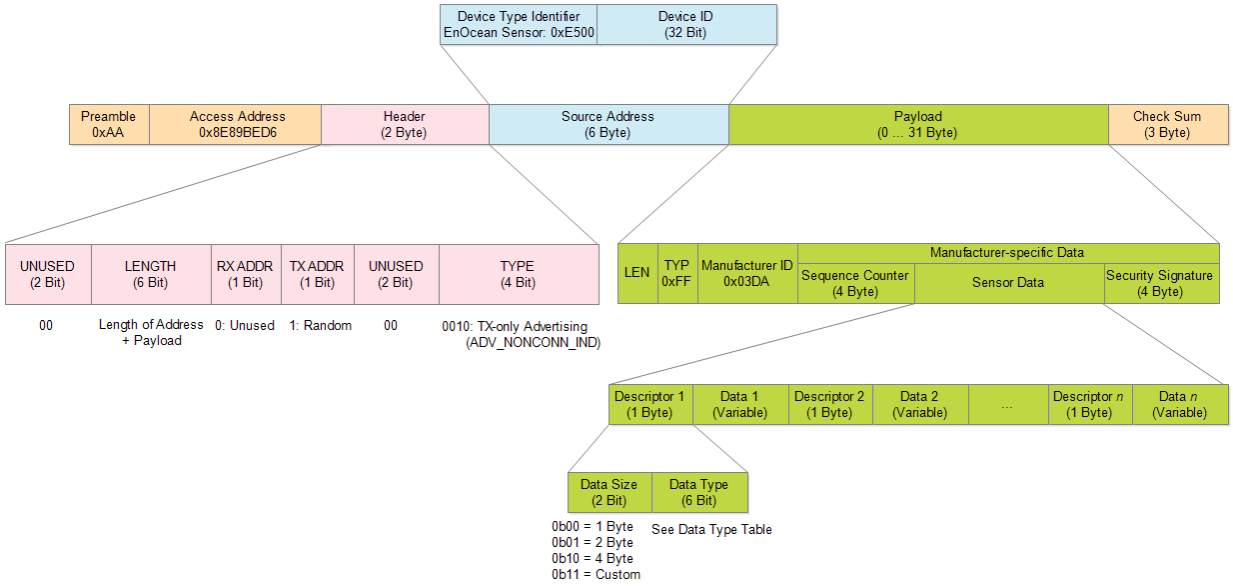

Figure 14 – BLE frame structure

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

6.1 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`.

6.2 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`.

6.3 Header

The BLE Header identifies certain radio telegram parameters. Figure 15 below shows the structure of the BLE header.

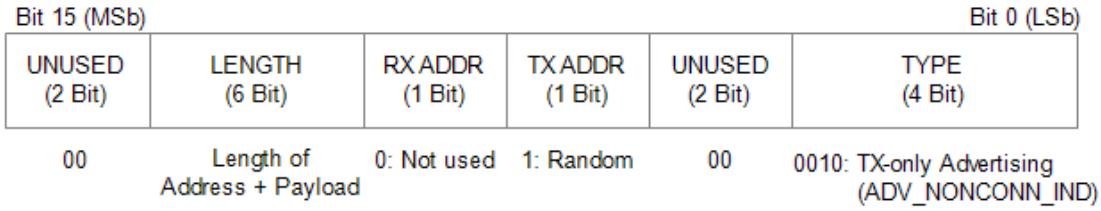

Figure 15 – BLE header structure

6.4 Source address

The 6 byte BLE Source Address (MAC address) uniquely identifies each EMDCB product. EMDCB supports two source address modes defined by the BLE standard:

- 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 `RPA` field in the SECURITY_CONFIG register to 0x01 as described in chapter 10.5.14.

6.4.1 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 modified via NFC as described in chapter 10.5.4.

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 filtering according to product type
- 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.

Figure 16 below illustrates the static address structure used by EMDCB.

Figure 16 – BLE static source address structure

6.4.2 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 modified via the NFC configuration interface as described in chapter 10.5.12.

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 17 below.

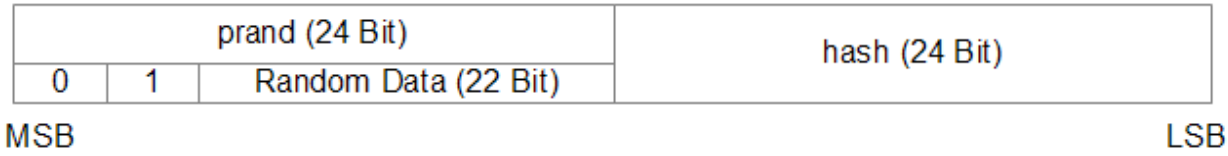

Figure 17 – BLE private resolvable source address structure

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 18 below illustrates the address resolving scheme for random private addresses.

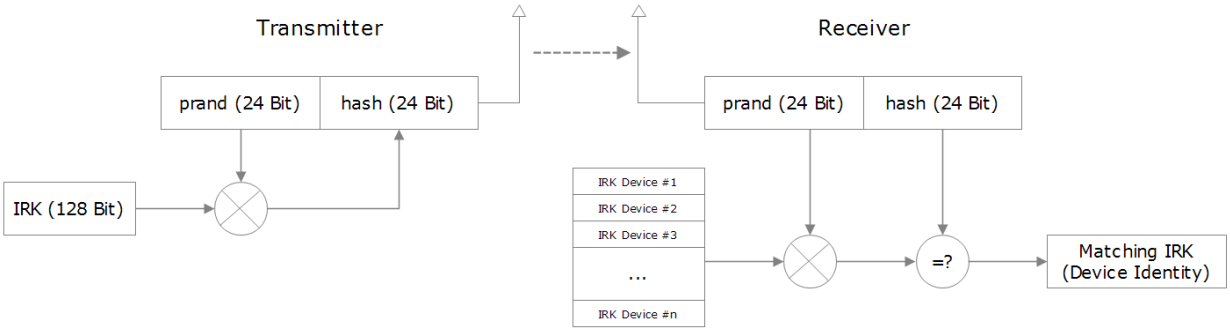

Figure 18 – Resolving private source addresses

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

Note that commissioning telegrams – as described in chapter 8.1 – will always use Static Source Addresses since they provide the identity resolution key required for resolving resolvable private addresses to the receiver.

6.5 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.

6.6 Payload

The payload of EnOcean BLE sensor data telegrams can 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 whenever a telegram (data telegram or commissioning telegram) is 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 6.6.1.

- Security Signature (4 byte)
  The *Security Signature* is used to authenticate EnOcean BLE sensor data telegrams, see chapter 7.

Figure 19 below illustrates the general telegram payload structure.

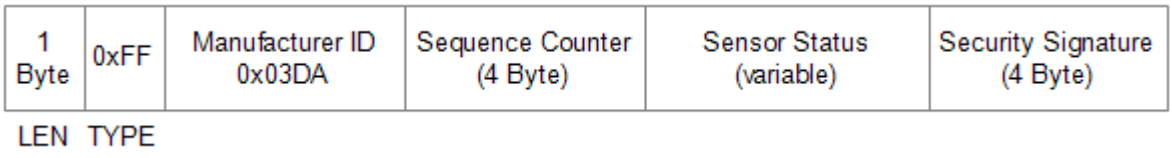

Figure 19 – Telegram payload structure

6.6.1 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 20 below shows the structure of the sensor status field.

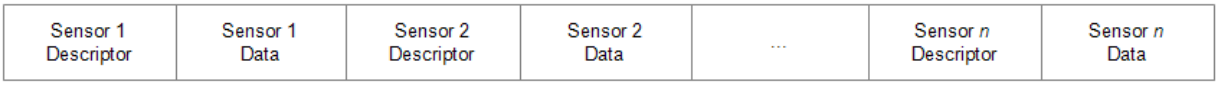

Figure 20 – Sensor Status field structure

6.6.2 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 21 below.

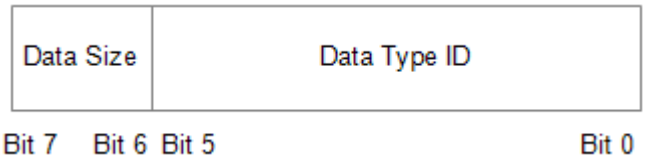

Figure 21 – Sensor Data Descriptor field structure

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).

6.6.3 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

6.7 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 (sensor)	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	Backup battery voltage	2	Disabled	-16383	16383	0.5	mV	2*x
0x02	Energy level	1	Enabled	0	100	0.5	%	2*x (0…200)
0x04	Light level (Solar cell)	2	Enabled	0	65 533	1	lx	1*x
0x3C	Optional Data	Variable	Disabled	User-defined data (Size defined by *profDesc*)				

Table 3 – Supported parameters

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.

7 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 22 below and exchanged as part of the radio telegram.

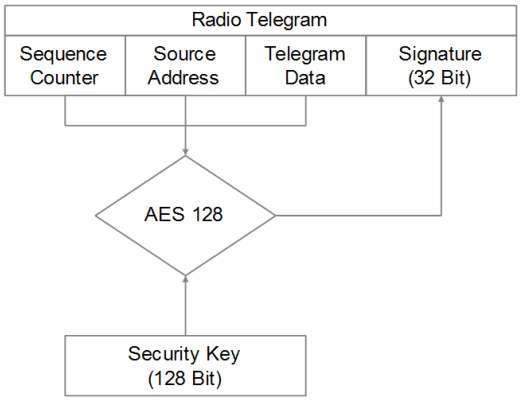

Figure 22 – Telegram authentication flow

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).

7.1 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 23 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 23 – 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 24 below.

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

Figure 24 – Authenticated payload

The calculated 32 bit signature is then appended to the data telegram payload as shown in in chapter 6.6

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.

8 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 as described in chapter 4.1.

- 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.

8.1 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 5.3.

Commissioning telegrams will always use static source addresses mode as discussed in chapter 6.4.1; using resolvable private addresses for commissioning telegrams is not possible since they contain the security key required for resolving those addresses.

The transmission of the commissioning telegram is triggered by pressing the LRN button as described in chapter 4.1.

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

8.2 QR code commissioning

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

8.2.1 Device label

The structure of the EMDC device label is shown in Figure 25 below.

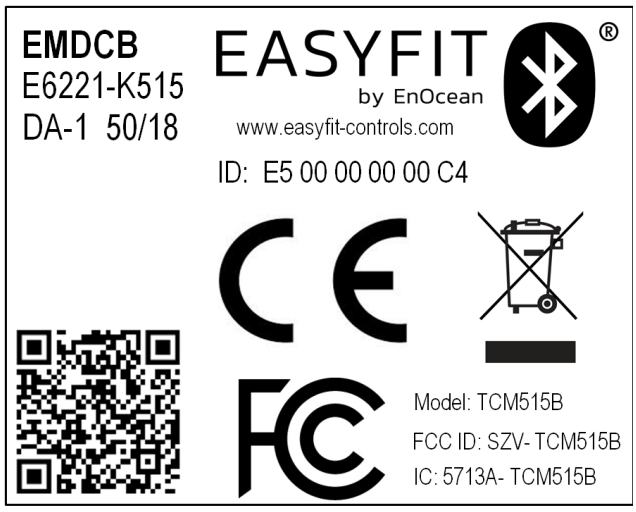

Figure 25 – EMDCB device label

8.2.2 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 26 shows an example of such QR code.

Figure 26 – EMDCB Commissioning QR code

8.2.3 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 26 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 chapter7.

8.3 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 10.5.4 and 10.5.12 respectively.

9 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 chapter 10.

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.

9.1 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.

9.2 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 the SET_NFC_PIN_CODE register as described in chapter 10.5.3.

9.3 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

9.3.1 USB NFC reader

For PC applications, EnOcean recommends the TWN4 Multitech 2 HF NFC Reader (order code T4BT-FB2BEL2-SIMPL) from Elatec RFID Systems (sales-rfid@elatec.com).
This reader is shown in Figure 27 below.

Figure 27 – Elatec TWN4 MultiTech Desktop NFC Reader with CDC interface

9.3.2 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.

9.4 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.

9.4.1 NFC interface state machine

Figure 28 below shows the overall state machine of the NFC interface.

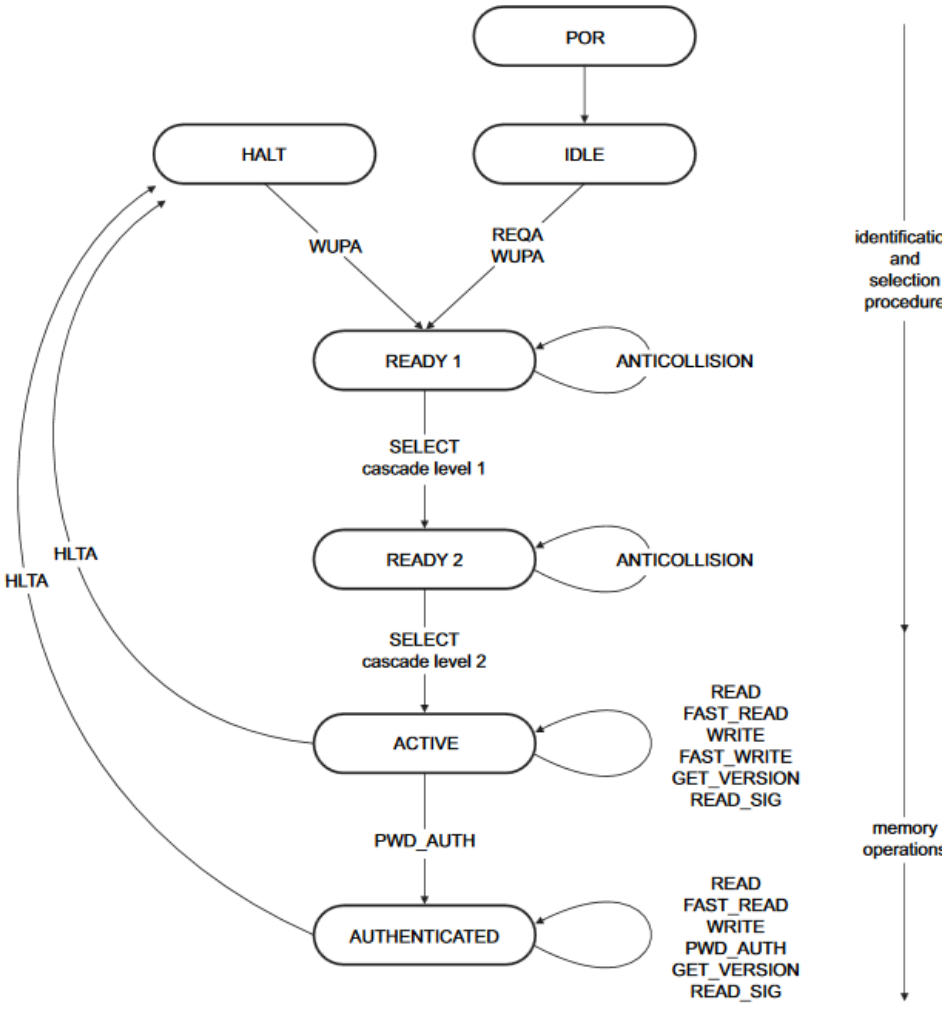

Figure 28 – NFC interface state machine

9.4.2 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.

9.4.3 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.

9.4.4 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.

9.4.5 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 NFC PIN code.

9.4.6 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 29 below shows the read command sequence.

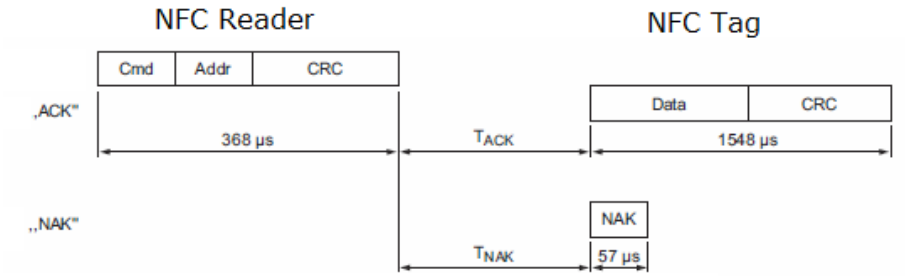

Figure 29 – NFC read command sequence

9.4.7 Write command

The WRITE command requires a start page address and writes 4 bytes of data into that page. Figure 30 below shows the read command sequence.

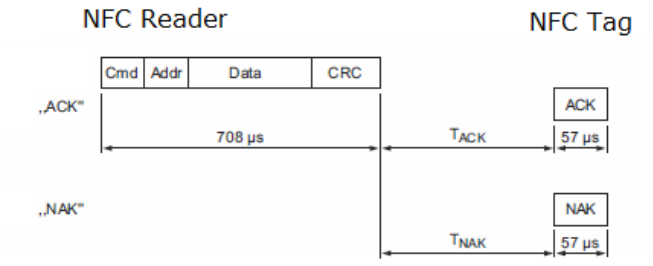

Figure 30 – NFC write command sequence

9.4.8 PWD_AUTH command (NFC PIN code authentication)

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

The PWD_AUTH command takes the 32 bit NFC PIN code as parameter and, if successful, returns the password authentication acknowledge, PACK.

Figure 31 below shows the password authentication sequence.

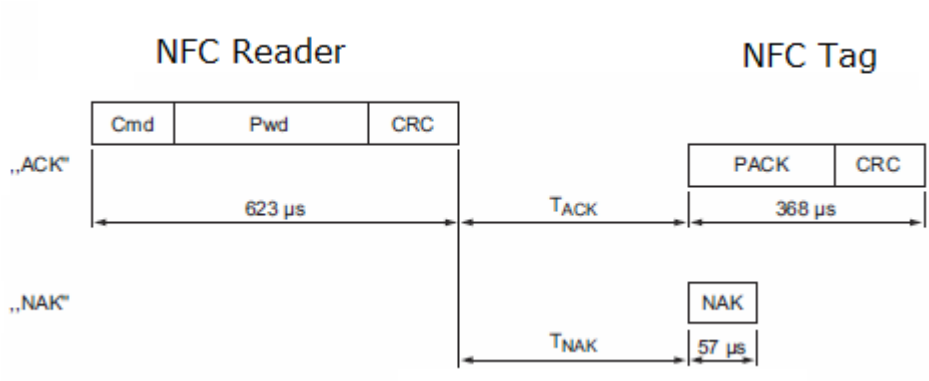

Figure 31 – Password authentication sequence

10 NFC registers

The NFC memory is organized in pages (smallest addressable unit) where each page contains 4 byte of data. Several pages with similar functionality form an NFC memory area.

10.1 NFC memory areas

These NFC pages are allocated into the following areas:

- NDEF (Public read-only access; no PIN required)
  This area contains an NDEF string identifying key device parameters
- PUBLIC INFO (Public read-only access; no PIN required)
  This area contains key device parameters in binary format
- NFC HEADER (Public read-only access; no PIN required)
  This area contains information about the NFC revision
- INTERNAL DATA (Non-accessible)
  This area contains calibration values and internal parameters and cannot be used
- CONFIGURATION (Read and Write access, PIN required)
  This area contains device configuration registers
- USER DATA (Read and Write access, PIN required)
  This area allows the user to store up to 64 byte of data.
  EMDCB does not use this area and does not interpret its content in any way.

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

NFC Address	Memory Area	Content
0x00 … 0x1A	NDEF	NDEF Device identification string (read-only)
0x1B … 0x23	PUBLIC INFO	Key device parameters (read-only)
0x24 … 0x26	NFC HEADER	NFC memory revision (read-only)
0x27 … 0x3F	INTERNAL DATA	Internal data (Do not use)
0x40 … 0x4E	CONFIGURATION	Configuration registers (Read / Write, PIN protected)
0x4F … 0xCF	INTERNAL DATA	Internal data (Do not use)
0xD0 … 0xDF	USER DATA	User data (64 byte read / write access, PIN protected)
0xE0 … 0xEB	INTERNAL DATA	Internal data (Do not use)

Table 5 – EMDCB NFC memory areas

10.2 NDEF

The NDEF area contains a device identification string using the NDEF (NFC Data Exchange Format) standard that is readable by most NFC-capable reader devices (including smartphones).

An example device identification string from the NDEF area of EMDCB would be:

```
30SE500000006DF+Z4BBE99C695FB5AB91DB8499E9206EE6F+30PE6221-K515+2PDA04+3C24
```

This NDEF string encodes the parameters shown in Table 6 below.

Identifier	Length of data (excl. identifier)	Value
30S	12 characters	Static Source Address (6 byte, variable)
Z	32 characters	Security Key (16 byte, variable)
30P	10 characters	Ordering Code (E6221-K515)
2P	4 characters	Step Code and Revision (DA04)
3C	2 characters	Header Offset (24)

Table 6 – NDEF Parameters

Note that the security key is only available if the Security Key Access in the Security Configuration register is set to 0b00: Public Access as described in chapter 10.5.13. Otherwise the security key will be listed as all zeros.

10.3 PUBLIC INFO

The PUBLIC INFO area provides the settings of several key configuration registers in hexa-decimal format.

10.3.1 PUBLIC_INFO area structure

Table 7 below shows the structure of the PUBLIC_INFO area.

NFC Address	Content			
	Byte 0	Byte 1	Byte 2	Byte 3
0x1B	SW_VERSION			
0x1C	SOURCE_ADDRESS			
0x1D	CH_REG1	CH_REG2	CH_REG3	TX_CFG
0x1E	TX_POWER	ADV_INTERVAL	MANUFACTURER_ID	
0x1F	OPTIONAL_DATA			
0x20 … 0x23	SECURITY_KEY (128 Bit) All zero if security key is private or protected			

Table 7 – PUBLIC INFO area structure

The registers in this area are described in more detail below.

10.3.2 SW_VERSION

The SW_VERSION register contains information about the version of the EMDCB device firmware.

The SW_VERSION register is organized as a sequence of 4 byte in the following order:

- Major revision (Byte 0)
- Minor revision (Byte 1)
- Major sub-revision (Byte 2)
- Minor sub-revision (Byte 3)

If the value in SW_VERSION would be 0x01020304 then the corresponding SW version would be 1.2.3.4.

10.3.3 Shadowed CONFIGURATION registers

The following registers of the CONFIGURATION area are shadowed in the PUBLIC_INFO area:

- SOURCE_ADDRES
- CH_REG1, CH_REG2, CH_REG3
- TX_CFG
- TX_POWER
- ADV_INTERVAL
- MANUFACTURER_ID
- OPTIONAL_DATA
- SECURITY_KEY

These registers can only be read in the PUBLIC_INFO; they can be read and written in the CONFIGURATION area after providing the correct PIN code. Please see chapter 10.5 for the description of these registers.

Note that public read access (without providing the correct PIN code) to the security key can be disabled using the KEY_ACCESS register as described in chapter 10.5.13.

10.4 NFC HEADER

The NFC HEADER area contains information about the NFC memory structure and can therefore be used to distinguish between different NFC memory layouts.

10.4.1 NFC HEADER area structure

The structure of the NFC HEADER area is shown in Figure 32 below.

NFC Address	Content			
	Byte 0	Byte 1	Byte 2	Byte 3
0x24	START (0xE0)	LENGTH (0x0A)	VERSION (0x01)	OEM MSB (0x00)
0x25	OEM LSB (0x0B)	DEVICE_IDENTIFIER (0x0B0002)		
0x26	REVISION (0x02)	END (0xFE)	UNUSED (0x0000)	

Figure 32 – NFC HEADER area structure

The NFC HEADER contains the following fields:

- START
  This field identifies the start of the NFC header and is always set to 0xE0
- LENGTH
  This field identifies the length of the NFC header.
  For EMDCB, this field is set to 0x0A since the header structure is 10 bytes long
- VERSION
  This field identifies the major revision and is set to 0x01 currently
- OEM
  The 16 bit OEM field identifies the manufacturer of the device so that manufacturer-specific layout implementations can be determined.
  For EnOcean GmbH this field is set to 0x000B
- DEVICE_IDENTIFIER
  The 24 bit DEVICE_IDENTIFIER field identifies an individual device from the range of devices manufactured by the manufacturer specified in the OEM field.
  For EMDCB, the DEVICE_IDENTIFIER is set to 0x0B0002
- REVISION
  The REVISION field identifies the exact revision of the NFC layout. This REVISION will be incremented whenever a change to the NFC layout is made.
- END
  The END field identifies the end of the NFC header and is always set to 0xFE. The number of bytes from START to END must equal LENGTH, otherwise the NFC header is invalid.

10.5 CONFIGURATION

The CONFIGURATION area allows configuring the device parameters and is therefore the most important part of the NFC memory.

Read or write access to the CONFIGURATION area is only possible after issuing a PWD_AUTH command as described in chapter 9.4.8 using the correct 32 bit PIN code.

10.5.1 CONFIGURATION area structure

The structure of the CONFIGURATION area is shown in Figure 32 below.

NFC Address	Content			
	Byte 0	Byte 1	Byte 2	Byte 3
0x40	SOURCE_ADDRESS			
0x41	CH_REG1	CH_REG2	CH_REG3	TX_CFG
0x42	TX_POWER	ADV_INTERVAL	MANUFACTURER_ID	
0x43	OPTIONAL_DATA			
0x44 … 0x47	SECURITY_KEY (128 Bit) All zero if security key access is disabled			
0x48	SECURITY_KEY_ACCESS	SECURITY_CFG	RFU	
0x49	REPORTING_CFG	OPTIONAL_DATA_SIZE	LED_MODE	FUNCTIONAL_MODE
0x4A	UNOCCUPIED_TX_INTERVAL		OCCUPIED_TX_INTERVAL	
0x4B	NFC_PIN_CODE			
0x4C	THRESHOLD_CFG	RFU		
0x4D	SOLAR_CELL_THRESHOLD		SOLAR_CELL_TX_INTERVAL	
0x4E	LIGHT_SENSOR_THRESHOLD		LIGHT_SENSOR_TX_INTERVAL	

Figure 33 – CONFIGURATION area structure

10.5.2 CONFIGURATION registers shadowed in PUBLIC_INFO area

The content of the following registers from the CONFIGURATION area (where read and write access is available) are copied into the PUBLIC_INFO area (with read-only access only):

- SOURCE_ADDRES
- CH_REG1, CH_REG2, CH_REG3
- TX_CFG
- TX_POWER
- ADV_INTERVAL
- MANUFACTURER_ID
- OPTIONAL_DATA
- SECURITY_KEY

Change made to these registers in the CONFIGURATION area will be copied to the PUBLIC_INFO area.

Specifically for the security key, this shadow copy feature can be disabled using the SECURITY_KEY_ACCES register as described in chapter 10.5.13.

10.5.3 NFC_PIN_CODE

The PIN code used to protect access to the NFC CONFIGURATION memory area should be changed from the default value to a user-specific value to avoid unauthorized access to the device configuration.

To do so, first authenticate with the current PIN code and then write the new PIN code (32 bit value) to the NFC_PIN_CODE register.

10.5.4 SOURCE_ADDRESS

Each EMDCB device uses a unique 6 byte address (Static Source Address) to identify its messages. This address is assigned during manufacturing.

The two most significant byte of this address are always 0xE500; i.e. the address always starts with 0xE500. The four least significant byte of this address can be read from the SOURCE_ADDRESS register.

The 6 byte address can then be calculated as (0xE500 << 32) + SOURCE_ADDRESS

10.5.5 CH_REG1, CH_REG2, CH_REG3

The channel selection registers CH_REG1, CH_REG2 and CH_REG3 define the radio channels for user-defined radio transmission sequences as described in chapter 5.3. The encoding of the radio channels follows the definition listed in Table 2.

10.5.6 TX_CFG

The transmission configuration register TX_CFG identifies the custom radio transmission sequence type (encoded by the bit field CHANNEL_MODE) and the data rate (encoded by the bit field DATA_RATE).

TX_CFG							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RFU		DATA_RATE		CHANNEL_MODE			

Figure 34 – TX_CFG register

The encoding for CHANNEL_MODE is shown Table 8 below.

CHANNEL_MODE	**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
0b0111 … 0b1111	Unused, will be treated as 0b0000

Table 8 – CHANNEL_MODE bit field encoding

The encoding for the DATA_RATE bit field is shown in Table 9 below.

DATA_RATE	**Data Rate**
0b00 (Default)	1 Mbit/s data rate
0b01	2 Mbit/s data rate
0b10, 0b11	Reserved, do not use

Table 9 – DATA_RATE bit field encoding

10.5.7 TX_POWER

The register TX_POWER identifies the transmission power used by EMDCB. Figure 35 below shows the structure of the TX_POWER register.

TX_POWER							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RFU						POWER	

Figure 35 – TX_POWER register

The encoding for the POWER bit field is shown in Table 10 below.

POWER	**Transmission Power**
0b00 (Default)	+4 dBm
0b01	0 dBm
0b10, 0b11	Reserved, do not use

Table 10 – POWER bit field encoding

10.5.8 ADV_INTERVAL

The register ADV_INTERVAL identifies the interval between consecutive advertising events. Figure 36 below shows the structure of the ADV_INTERVAL register.

ADV_INTERVAL							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RFU						INTERVAL	

Figure 36 – ADV_INTERVAL register

The encoding for the INTERVAL bit field is shown in Table 11 below.

INTERVAL	**Advertising Interval**
0b00 (Default)	20 ms
0b01	10 ms
0b10, 0b11	Reserved, do not use

Table 11 – INTERVAL bit field encoding

10.5.9 MANUFACTURER_ID

The register MANUFACTURER_ID identifies the manufacturer of the device using the 16 bit company identifier assigned by Bluetooth SIG. The default setting of 0x03DA identifies EnOcean GmbH as the manufacturer of the device.

At the time of writing, the list of assigned company identifiers could be found here:
https://www.bluetooth.com/specifications/assigned-numbers/company-identifiers/

10.5.10 OPTIONAL_DATA

The register OPTIONAL_DATA identifies additional (up to 4 byte) of user-defined data that can be transmitted as part of each data telegram. This data can be used to convey additional information about the use of EMDCB and is user-defined.

The amount of OPTIONAL_DATA to be transmitted (0, 1, 2 or 4 byte) is determined by the OPTIONAL_DATA_SIZE register described below.

10.5.11 OPTIONAL_DATA_SIZE

The OPTIONAL_DATA_SIZE register determines how many user-defined data bytes from the OPTIONAL_DATA register will be transmitted as part of data telegrams.

Figure 40 below shows the structure of the OPTIONAL_DATA_SIZE register.

OPTIONAL_DATA_SIZE							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RFU						SIZE	

Figure 37 – OPTIONAL_DATA_SIZE register

The encoding used by the SIZE bit field is shown in Table 12 below.

SIZE	**Optional Data Size**
0b00 (Default)	No optional data reported
0b01	1 byte optional data reported (Byte 0 of OPTIONAL_DATA)
0b10	2 byte optional data reported (Byte 0 and Byte 1 of OPTIONAL_DATA)
0b10	4 byte optional data reported (Byte 0 … Byte 3 of OPTIONAL_DATA)

Table 12 – SIZE bit field encoding

10.5.12 SECURITY_KEY

The register SECURITY_KEY identifies the 16 byte security key used to authenticate the data telegrams of EMDCB.

Access to the SECURITY_KEY via this register or via its copy in the NDEF ore PUBLIC INFO area can be disabled by the user via the SECURITY_KEY_ACCESS register described below.

10.5.13 SECURITY_KEY_ACCESS

The register SECURITY_KEY_ACCESS allows protecting access to the device-unique security key via the SECURITY_KEY field of the NFC interface or via the transmission of a LRN telegram as described in chapter 8.1.

Figure 38 below shows the structure of the SECURITY_KEY_ACCESS register.

SECURITY_KEY_ACCESS							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RFU					LRN_TEL_ACCESS	NFC_ACCESS	

Figure 38 – SECURITY_KEY_ACCESS register

The encoding for the NFC_ACCESS bit field is shown in Table 13 below.

NFC_ACCESS	**Access to security key via NFC**
0b00 (Default)	Public NFC Access: Security key visible in NFC, No NFC PIN required
0b01	Private NFC Access: Security key visible in NFC, NFC PIN required
0b10	No NFC Access: Security key not visible in NFC
0b10	Reserved, do not use

Table 13 – NFC_ACCESS bit field encoding

The encoding for the LRN_TEL_ACCESS bit field is shown in Table 14 below.

LRN_TEL_ACCESS	**Access to security key via LRN telegram**
0b0 (Default)	LRN Telegram (containing security key) enabled
0b1	LRN Telegram (containing security key) disabled

Table 14 – LRN_TEL_ACCESS bit field encoding

10.5.14 SECURITY_CFG

The SECURITY_CFG register allows the configuration of the security parameters used by EMDCB.
Figure **39** below shows the structure of the SECURITY_CFG register.

SECURITY_CFG							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RFU			RPA	SECURITY_MODE			

Figure 39 – SECURITY_CFG register

The encoding for the SECURITY_MODE bit field is shown in Table 15 below.

EMDCB currently always uses authentication with a 32 bit sequence counter generating a 32 bit message integrity code (MIC) based on a 128 bit random device-unique security key. Other security modes might be added in the future.

SECURITY_MODE	**Security Mode**
`0b0000 (Default)`	Authentication with 32 bit sequence counter and 32 bit MIC
`Others`	Reserved (do not use)

Table 15 – SECURITY_MODE bit field encoding

EMDCB uses by default a device-unique static source address (constant throughout the life-time of the device) starting with 0xE500 as described in chapter 6.4.1.

EMDCB can alternatively use a resolvable private address (RPA) to obfuscate the origin of its data telegrams as described in chapter 6.4.2.

The selection between these two modes is done using the RPA bit field as shown in Table 16 below.

RPA	**Address Mode**
`0b0 (Default)`	Use Static Source Address
`0b1`	Use Resolvable Private Address (RPA)

Table 16 – RPA bit field encoding

10.5.15 REPORTING_CFG

The REPORTING_CFG register determines which items are transmitted within data telegrams. Figure 40 below shows the structure of the REPORTING_CFG register.

REPORTING_CFG							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RFU					SOLAR_CELL	ENERGY	

Figure 40 – REPORTING_CFG register

The ENERGY bit field allows selecting if the voltage of the backup battery and / or the energy level of the internal energy store containing the harvested energy is reported. The encoding for the ENERGY bit field is shown in Table 17 below.

ENERGY	**Harvested Energy / Backup Battery Voltage Reporting**
0b00	Disabled: No reporting of energy
0b01 (Default)	Adaptive: Backup battery voltage if present, else harvested energy
0b10	Harvested: Always report harvested energy
0b11	Both: Report backup battery voltage and harvested energy

Table 17 – ENERGY bit field encoding

The SOLAR_CELL bit field determines if the illumination of the solar cell is reported within data telegrams. The encoding for the SOLAR_CELL bit field is shown in Table 18 below.

SOLAR_CELL	**Solar Cell Illumination Reporting**
0b0	Disabled: Do not report solar cell illumination
0b1 (Default)	Enabled: Report solar cell illumination

Table 18 – SOLAR_CELL bit field encoding

10.5.16 LED_MODE

The LED_MODE register determines the brightness of the LED and allows disabling LED notification for telegrams reporting "occupied" (motion detected) status. Figure 41 below shows the structure of the LED_MODE register.

LED_MODE							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RFU						LED	

Figure 41 – LED_MODE register

The encoding used by the LED bit field is shown in Table 19 below.

LED	**LED Intensity**
0b00	LED is disabled
0b01	Low intensity
0b10 (Default)	Medium intensity
0b11	Maximum intensity

Table 19 – LED bit field encoding

10.5.17 FUNCTIONAL_MODE

The FUNCTIONAL_MODE register can be used to switch between standard operation mode and Standby (Sleep) mode as described in chapter 2.5. Figure 42 below shows the structure of the FUNCTIONAL_MODE register.

FUNCTIONAL_MODE							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RFU				MODE			

Figure 42 – FUNCTIONAL_MODE register

The encoding used by the MODE bit field is shown in Table 20 below.

MODE	**Functional Mode**
0b0000 (Default)	Standard Operation Mode
0b0001	Standby (Sleep) Mode
Others	Reserved (Do not use)

Table 20 – MODE bit field encoding

10.5.18 UNOCCUPIED_TX_INTERVAL

The reporting interval used while no motion is detected is set by the register UNOCCUPIED_TX_INTERVAL shown in Figure 43 below.

UNOCCUPIED_TX_INTERVAL				
Bit 15	Bit 14	…	Bit 1	Bit 0
UNOCCUPIED INTERVAL				

Figure 43 – UNOCCUPIED_TX_INTERVAL register

The encoding used by the UNOCCUPIED INTERVAL bit field is shown in Table 21 below.

UNOCCUPIED INTERVAL	**Standard Reporting Interval**
`0x0000, 0x0001, 0x0002`	Not supported (Do not use)
`0x0003`	3 seconds (minimum setting)
…	…
`0x0078 (Default)`	120 seconds (default setting)
…	…
`0xFFFF`	65535 seconds (maximum setting)

Table 21 – UNOCCUPIED INTERVAL bit field encoding

10.5.19 OCCUPIED_TX_INTERVAL

The reporting interval used while no motion is detected is set by the register OCCUPIED_TX_INTERVAL shown in Figure 44 below.

OCCUPIED_TX_INTERVAL				
Bit 15	Bit 14	…	Bit 1	Bit 0
OCCUPIED INTERVAL				

Figure 44 – OCCUPIED_TX_INTERVAL register

The encoding used by the OCCUPIED INTERVAL bit field is shown in Table 22 below.

OCCUPIED INTERVAL	**Occupancy-based Reporting Interval**
0x0000, 0x0001, 0x0002	Not supported (Do not use)
0x0003	3 seconds (minimum setting)
…	…
0x003C (Default)	60 seconds (default setting)
…	…
0xFFFF	65535 seconds (maximum setting)

Table 22 – OCCUPIED INTERVAL bit field encoding

The default reporting interval while motion (occupancy) is detected is 60 seconds.

If no reporting interval reduction is desired for the case when a room is occupied, then set OCCUPIED_TX_INTERVAL to the same value as UNOCCUPIED_TX_INTERVAL (which by default is 120 seconds).

10.5.20 THRESHOLD_CFG

The reporting interval of EMDCB is determined by the register UNOCCUPIED_TX_INTERVAL (if not motion is detected) or by the register OCCUPIED_TX_INTERVAL (if motion is detected).

It is possible to reduce the reporting interval from based on available light for the solar cell or the light level measured by the light level sensor. This mechanism is called illumination-controlled reporting interval and is described in chapter 2.6.3.

The use of the illumination-controlled reporting interval is enabled by the THRESHOLD_CFG register shown in Figure 45 below.

THRESHOLD_CFG							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RFU				LIGHT SENSOR		SOLAR CELL	

Figure 45 – THRESHOLD_CFG register

The encoding used by both the SOLAR CELL bit field is shown in Table 23 below.

SOLAR CELL	**Reporting Interval Reduction (Solar Cell)**
0b00 (Default)	Disabled (No reporting interval reduction)
0b01	Reserved (Do not use)
0b10	Enabled (Reporting interval reduction if light above threshold)
0b11	Reserved (Do not use)

Table 23 – SOLAR CELL bit field encoding

The encoding used by both the LIGHT SENSOR bit field is shown in Table 24 below.

LIGHT SENSOR	**Reporting Interval Reduction (Light Sensor)**
0b00 (Default)	Disabled (No reporting interval reduction)
0b01	Reserved (Do not use)
0b10	Enabled (Reporting interval reduction if light above threshold)
0b11	Reserved (Do not use)

Table 24 – LIGHT SENSOR bit field encoding

10.5.21 SOLAR_CELL THRESHOLD

If reduction of the reporting interval based on the solar cell light level has been enabled then the light level threshold is defined by SOLAR_CELL_THREHOLD register as shown in Figure 46 below.

SOLAR_CELL_THRESHOLD				
Bit 15	Bit 14	…	Bit 1	Bit 0
SOLAR THRESHOLD				

Figure 46 – SOLAR_CELL_THRESHOLD register

The encoding used by the SOLAR THRESHOLD bit field is shown in Table 22 below.

SOLAR THRESHOLD	**Threshold**
0x0000	0 lux (minimum setting)
…	…
0x00C8 (Default)	200 Lux seconds (default setting)
…	…
0xFFFF	65535 lux (maximum setting)

Table 25 – SOLAR THRESHOLD bit field encoding

The default setting for the solar cell threshold is 200 lux which corresponds to good availability of ambient light for harvesting.

10.5.22 SOLAR_CELL_TX_INTERVAL

If solar cell illumination-controlled reporting has been enabled and the solar cell illumination is above the defined threshold then the resulting reporting interval will be determined by the register SOLAR_CELL_TX_INTERVAL shown in Figure 47 below.

SOLAR_CELL_TX_INTERVAL				
Bit 15	Bit 14	…	Bit 1	Bit 0
SOLAR INTERVAL				

Figure 47 – SOLAR_CELL_TX_INTERVAL register

The encoding used by the SOLAR INTERVAL bit field is shown in Table 26 below.

SOLAR INTERVAL	**Solar cell illumination-based reporting interval**
0x0000, 0x0001, 0x0002	Not supported (Do not use)
0x0003	3 seconds (minimum setting)
…	…
0x0078 (Default)	120 seconds (default setting)
…	…
0xFFFF	65535 seconds (maximum setting)

Table 26 – SOLAR INTERVAL bit field encoding

The default reporting interval while solar cell illumination is above the solar cell illumination threshold is 120 seconds. This can be reduced according to user requirements keeping in mind the energy balance.

As a guidance, for a light level of 200 lux it should be possible to reduce the reporting interval to 60 seconds.

10.5.23 LIGHT_SENSOR_THRESHOLD

If reduction of the reporting interval based on the light level measured by the light sensor has been enabled then the light level threshold is defined by LIGHT_SENSOR_THREHOLD register as shown in Figure 48 below.

LIGHT_SENSOR_THRESHOLD				
Bit 15	Bit 14	…	Bit 1	Bit 0
LIGHT SENSOR THRESHOLD				

Figure 48 – LIGHT_SENSOR_THRESHOLD register

The encoding used by the LIGHT SENSOR THRESHOLD bit field is shown in Table 27 below.

LIGHT SENSOR THRESHOLD	**Threshold**
0x0000	0 lux (minimum setting)
…	…
0x00C8 (Default)	200 Lux seconds (default setting)
…	…
0xFFFF	65535 lux (maximum setting)

Table 27 – LIGHT SENSOR THRESHOLD bit field encoding

The default setting for the light sensor threshold is 200 lux.

10.5.24 LIGHT_SENSOR_TX_INTERVAL

If solar cell illumination-controlled reporting has been enabled and the solar cell illumination is above the defined threshold then the resulting reporting interval will be determined by the register LIGHT_SENSOR_TX_INTERVAL shown in Figure 49 below.

LIGHT_SENSOR_TX_INTERVAL				
Bit 15	Bit 14	…	Bit 1	Bit 0
LIGHT SENSOR INTERVAL				

Figure 49 – LIGHT_SENSOR_TX_INTERVAL register

The encoding used by the LIGHT SENSOR INTERVAL bit field is shown in Table 28 below.

LIGHT SENSOR INTERVAL	Light sensor illumination-based reporting interval
0x0000, 0x0001, 0x0002	Not supported (Do not use)
0x0003	3 seconds (minimum setting)
…	…
0x0078 (Default)	120 seconds (default setting)
…	…
0xFFFF	65535 seconds (maximum setting)

Table 28 – LIGHT SENSOR INTERVAL bit field encoding

The default reporting interval while the light level measured by the light sensor is above the light sensor illumination threshold is 120 seconds. This can be reduced according to user requirements keeping in mind the energy balance.

As a guidance, for a measured light level of 200 lux it should be possible to reduce the reporting interval to 60 seconds.

10.6 USER DATA

The USER DATA area allows the user to read and write up to 64 byte of data after entering the correct PIN code. Typical use cases include storing information about the configuration or the installation of the device (by whom, when, what). EMDCB does not use this area and does not interpret its content in any way.

11 Installation recommendations

11.1 Motion detection

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 Wi-Fi 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.

11.2 Illumination measurement

The dedicated illumination sensor integrated into EMDCB accurately measures and report the light level directly underneath (e.g. on the desk surface) with a spectral response close to the human eye's perception of ambient light.

The following points should be considered when using the illumination sensor:

- Aperture
  The sensor measures the light level within a small radius directly underneath it. If the lighting conditions within that area are not representative for the overall conditions, then the result might be different from expectation.

- Surface
  The most common application for a ceiling-mounted illumination sensor is to measure the light level at a working desk surface underneath. In this application, the measured light level depends on the reflectivity of the surface
  Simply put, a dark desk surface will give a totally different result compared to a white desk surface even when the same luminous flow is directed towards it.

- Obstruction
  Any obstruction between the sensor and the intended measurement area (desk surface, window) will significantly impact the measurement result. Maintaining a clear line of sight between measurement area and illuminations sensor is therefore essential.

- Interference
  To ensure accurate measurement results, it is essential to minimize interference from other light sources not contributing to the illumination at the target measurement area.
  For instance, when measuring the light level at a desk surface, interference might occur due to direct light from the window or from or upwards emission of indirect light sources (floor lamps etc)

Consider using the light level reported by the solar cell as an alternative approach if measuring a light level over a wider area is desired.

11.3 Energy harvesting

EMDCB is powered by ambient light using its integrated solar cell. For best performance it is therefore essential to maximize the amount of light available for harvesting.

Harvestable light will typically be either natural light (daylight coming in through windows etc) or artificial light (direct or reflected light from indoor luminaires). If natural light is available (e.g. from a window) then the solar cell of EMDCB should be oriented as much as possible towards that.

As guidance it can be assumed that a light level of 200 lux at the desk surface will in most cases result in sufficient available light for operation of EMDCB with its standard parameters. The light level directly at the solar cell should be at least 50 lux for that.

Marginally lower levels of available can be addressed by configuring a lower reporting rate via NFC as discussed in chapter 2.6.

If the available light is insufficient then EMDCB offers the option for a CR2032 backup battery as described in chapter 4.5.

11.4 NFC configuration

EMDCB can be flexibly configured for a wide range of application scenarios using the NFC configuration interface as described in chapters 9 and 10.

Before making any configuration changes, be sure to familiarize yourself with the device functionality and determine the energy constraints based on the available ambient light. Be especially careful not to configure high update rates (low reporting intervals) before ensuring that sufficient light is available.

Should you be unsure about the current NFC configuration then execute a factory reset as described in chapter 4.3 to reset all configuration registers to their default setting.

After completing the NFC configuration and ensuring that all functionality works as required, it is recommended to lock the NFC configuration interface by changing the NFC PIN code from its default value to a different (secret) value. Make sure the new PIN code is properly noted down.

12 Regulatory notes

12.1 European Union

12.1.1 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

12.1.2 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

12.2 FCC (United States)

12.2.1 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.

12.2.2 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.

12.2.3 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.

12.2.4 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.

12.3 ISED (Industry Canada)

12.3.1 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
FVIN ▶ N/A

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

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

12.3.2 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.”

13 Product history

Table **29** 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
DA-04	December 2019	Addition of adaptive reporting via solar cell and light sensor

Table 29 – 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 30 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 30 – Advertising message parsing

A.1.2 Data telegram payload

The EnOcean payload can be parsed as shown in Table 31 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 31 – EnOcean data telegram payload parsing

A.1.3 Sensor data

The sensor data can be parsed as shown in Table 32 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 32 – 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 33 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 33 – Advertising data parsing

A.2.2 Commissioning telegram payload

The payload of the commissioning telegram can be parsed as shown in Table 34 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 34 – 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 8.2
- From the NFC configuration memory as described in chapter 9

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 35 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 35 – 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 36 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 36 – 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 37 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 37 – 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 38 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 38 – 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 50 below.

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

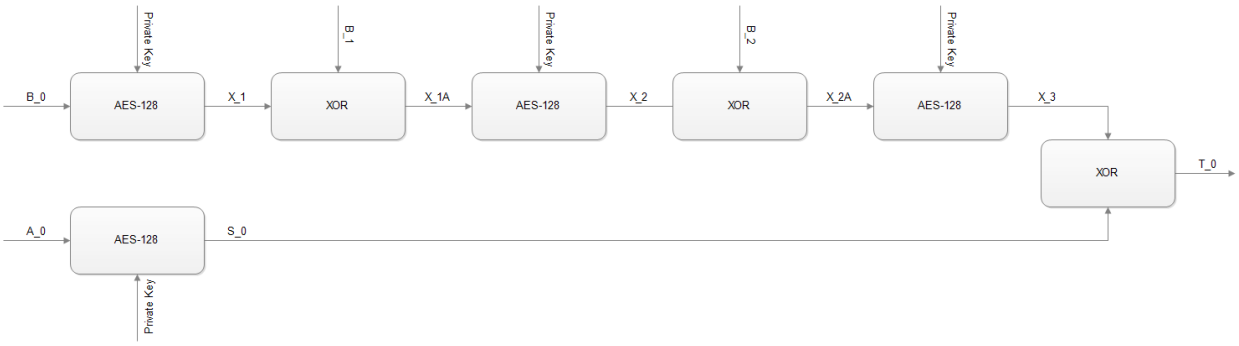

Figure 50 – RFC3610 execution sequence

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 50 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 6.4.2. 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 51 below.

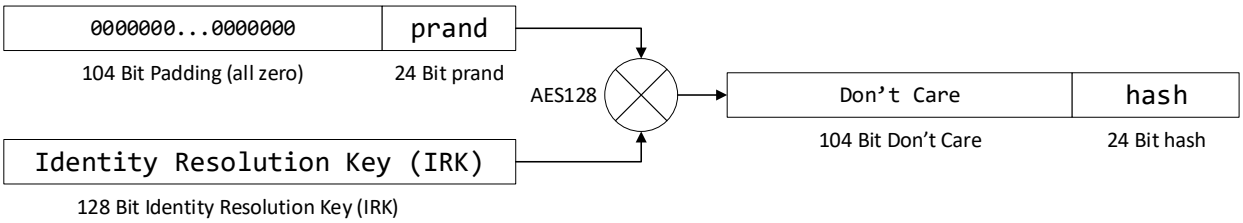

Figure 51 – Execution flow for resolving private addresses (RPA resolution)

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 10.5.12.

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 10.5
- From the device label as specified in chapter 8.2 (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 17, 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 6.4.2, the setting of `0b01` indicates resolvable private address mode.

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

```
0x000000000000000000000000493970
```

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;
                0x000000000000000000000000493970)
```

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.