

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

ESRPB / EDRPB

EASYFIT Bluetooth® Single / Double Rocker Pad

09.01.2018



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

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

REVISION HISTORY

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

Version	Author	Reviewer	Date	Major Changes
1.0	MKA	MKA	22.02.2017	Initial Release
1.1	MKA	MKA	30.03.2017	Added step by step payload parsing example
1.2	MKA	MKA	30.06.2017	Added product label information
1.3	MKA	MKA	09.01.2018	Added Australia approval

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

© EnOcean GmbH, All Rights Reserved

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.

Components of the modules are considered and should be disposed of as hazardous waste. Local government regulations are to be observed.

Packing: Please use the recycling operators known to you.

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

TABLE OF CONTENT

1	GENERAL DESCRIPTION	6
1.1	Basic functionality	6
1.2	Ordering information.....	6
1.3	Technical data.....	7
1.4	Physical dimensions and mounting options	7
1.5	Environmental conditions	7
1.6	Packaging information.....	7
2	FUNCTIONAL INFORMATION	8
2.1	Product Overview	8
3	Telegram transmission	9
3.1	Radio channel parameters	9
3.2	Default radio transmission sequence.....	10
3.3	User-defined radio transmission sequences.....	10
3.3.1	Three channel sequence	11
3.3.2	Two channel sequence.....	12
3.3.3	Single channel sequence.....	12
4	Telegram format	13
4.1	Preamble.....	13
4.2	Access Address	13
4.3	Header.....	13
4.4	Source address	14
4.4.1	Static source address mode	14
4.4.2	Private resolvable source address mode	15
4.5	Check Sum.....	16
4.6	Payload.....	17
4.7	Switch status encoding.....	18
4.8	ExRPB telegram authentication	19
4.8.1	Authentication implementation	20
5	ExRPB commissioning	21
5.1	NFC-based commissioning	22
5.2	Camera-based commissioning via QR code	23
5.2.1	QR code format	23
5.3	Radio-based commissioning.....	24
5.3.1	Commissioning mode entry.....	24
5.3.2	Commissioning telegram transmission.....	25
5.3.3	Exit from commissioning mode.....	26
5.4	Factory Reset.....	26
6	NFC interface	27
6.1	Using the NFC interface.....	27
6.2	NFC interface functions	28

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

6.2.1	NFC interface state machine.....	28
6.2.2	IDLE state.....	29
6.2.3	READY 1 state.....	29
6.2.4	READY 2 state.....	29
6.2.5	ACTIVE state.....	29
6.2.6	Read command	30
6.2.7	Write command	30
6.2.8	Password authentication (PWD_AUTH) command	31
6.3	Using TWN4 as USB NFC reader	32
6.3.1	Useful commands	33
6.3.2	Translation into binary data	33
6.4	Configuration memory organization	34
6.5	Memory Address Map.....	35
6.6	Public data	36
6.7	Protected Data	37
6.7.1	PIN Code	38
6.7.1	Configuration of product parameters	38
6.7.2	Source Address Write register	38
6.7.3	Security Key Write register	39
6.7.4	Product ID and Manufacturer ID Write register	40
6.7.5	Optional Data register	40
6.7.6	Configuration register.....	41
6.7.7	Custom Channel Mode register	42
6.7.8	Radio Channel Selection registers	43
6.7.9	Customer Data	44
6.8	Private Data.....	45
6.8.1	Security Key	45
6.8.2	Default Settings.....	45
7	Device Label	46
8	APPLICATION INFORMATION	47
8.1	Transmission range	47
8.2	External magnets	47
8.3	Receiver configuration.....	48
9	REGULATORY INFORMATION.....	49
9.1	CE / RE-D for Europe Union	49
9.2	FCC (United States) Certificate.....	50
9.2.1	FCC (United States) Regulatory Statement.....	51
9.3	IC (Industry Canada) Certificate.....	52
9.3.1	IC (Industry Canada) Regulatory Statement.....	53
9.4	ACMA (Australia) Declaration of Conformity	54
A	Parsing ESRPB / EDRPB radio telegrams.....	56
A.1	Data telegram example	56
A.1.1	BLE frame structure.....	56
A.1.2	EnOcean data telegram payload structure.....	56
A.2	Commissioning telegram example	57
A.2.1	BLE frame structure.....	57

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

A.2.2	EnOcean commissioning telegram payload structure	57
B	Authentication of ESRPB / EDRPB data telegrams	58
B.1	Algorithm input parameters	58
B.1.1	Constant input parameters	58
B.1.2	Variable input parameters	59
B.1.3	Obtaining the security key	60
B.1.3.1	Obtaining the security key via NFC interface.....	60
B.1.3.2	Obtaining the security key via the product DMC code	61
B.1.3.3	Obtaining the security key via a commissioning telegram.....	61
B.2	Internal parameters.....	62
B.3	Constant internal parameters.....	62
B.4	Variable internal parameters.....	63
B.5	Algorithm execution sequence.....	63
B.6	Examples	64
B.6.1	Data telegram without optional data	64
B.6.2	Data telegram with 1 byte optional data	66
B.6.3	Data telegram with 2 byte optional data	67
B.6.4	Data telegram with 4 byte optional data	68

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

1 GENERAL DESCRIPTION

1.1 Basic functionality

EnOcean Easyfit Bluetooth® Single / Double Rocker Pad (ESRPB / EDRPB, jointly referred to as ExRPB) are universal energy harvesting wireless switches in the US rocker pad form factor for systems using the 2.4 GHz Bluetooth Low Energy (BLE) radio standard.

ESRPB and EDRPB are based on the maintenance free, self-powered Bluetooth pushbutton transmitter module PTM 215B.

PTM 215B contains an electro-dynamic energy transducer which is actuated by the ExRPB rocker movement. Whenever a rocker is pushed down or released, electrical energy is created and a set of Bluetooth advertising frames is transmitted by the PTM 215B radio transmitter which identifies the rocker status (pushed or released).

ExRPB radio telegrams are protected with AES-128 security based on a device-unique private key.

„Long“ or „Short“ rocker press (the time between pushing and releasing the rocker) can be calculated by the receiver. This enables switching, dimming control or jalousie control including slat action

Figure 1 below shows the single rocker (ESRPB) and double rocker (EDRPB) product variants.



Figure 1 – ESRPB (single rocker) and EDRPB (double rocker) variants

1.2 Ordering information

Type	Ordering Code
ESRPB	ESRPB-W-EO
EDRPB	EDRPB-W-EO

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

1.3 Technical data

Antenna	Integrated PCB antenna
Output Power	0 dBm
Communication Range (Guidance Only)	75 m ideal line of sight / 10 m indoor environment
Communication Standard	Bluetooth Low Energy (Advertising)
Radio Frequency (min / max)	2402 MHz / 2480 MHz
Default Radio Channels	BLE CH 37 / 38 / 39 (2402 MHz / 2426 MHz / 2480 MHz)
Advertising Events per press or release (min / max)	2 / 3
Data Rate and Modulation	1 Mbit/s GFSK
Configuration Interface	NFC Forum Type 2 Tag (ISO/IEC 14443 Part 2 and 3)
Device Identification	Unique 48 Bit Device ID (factory programmed)
Security	AES128 (CBC Mode) with Sequence Code
Power Supply	Integrated Kinetic Energy Harvester
Inputs	Single (ESRPB) or Double Rocker (EDRPB)

1.4 Physical dimensions and mounting options

Dimensions of Single Rocker Pad	4.95" H x 3.21" W x 0.74" D (126mm x 82mm x 19mm)
Dimensions of Double Rocker Pad	4.95" H x 4.52" W x 0.72" D (126mm x 115mm x 18mm)
Weight of Single Rocker Pad	3.9 oz (112g)
Weight of Double Rocker Pad	5.3 oz (150g)
Mounting	Screwing onto flat surface (screws enclosed)

1.5 Environmental conditions

Operating Temperature	-25°C ... 65°C
Storage Temperature	-25°C ... 65°C
Humidity	0% to 95% r.h. (non-condensing)

1.6 Packaging information

Packaging Unit	24 units
Packaging Method	Each unit packed in a box, 24 units packed in a case

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

2 FUNCTIONAL INFORMATION

2.1 Product Overview

Easyfit Bluetooth Single (ESRPB) and Double (EDRPB) Rocker Pad from EnOcean enable the implementation of wireless switches in the US rocker pad form factor without batteries.

ESRPB and EDRPB are based on the PTM 215B energy harvesting wireless pushbutton module which is shown in Figure 2 below.



Figure 2 – PTM 215B module

Power is provided by an electro-dynamic energy generator that is built into the PTM 215B module and enables radio transmissions using the 2.4GHz Bluetooth Low Energy (BLE) standard.

The PTM 215B module provides four button contacts which are actuated by one (single) rocker (ESRPB) or two (double) rockers (EDRPB). The button contacts of the PTM 215B module are grouped into two channels (Channel A and Channel B) with each channel containing two button contacts (State O and State I).

For the double rocker variant EDRPB, each channel is actuated by one of the two rockers. In case of the single rocker variant ESRPB, only channel B is actuated by the single rocker. The state of all four button contacts (pressed or not pressed) is transmitted together with a unique device identification (48 bit source address) whenever a rocker is pushed or released.

Figure 3 below shows the arrangement of the four button contacts on the PTM 215B module and their designation.

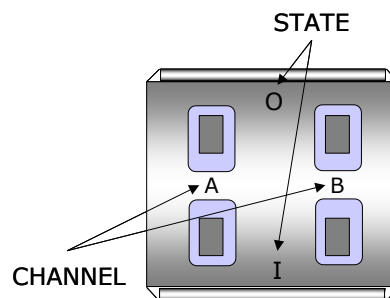


Figure 3 – Button contact designation of the PTM 215B module

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

3 Telegram transmission

3.1 Radio channel parameters

ExRPB transmits advertising telegrams within the 2.4 GHz radio frequency band (2402MHz ... 2480MHz) using the Bluetooth Low Energy (BLE) advertising frame format.

By default, ExRPB 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, see chapter 6.7.8.

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 1 below summarizes radio channels supported by ExRPB.

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 1 – ExRPB supported radio channels

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

3.2 Default radio transmission sequence

ExRPB 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, ExRPB will send several (minimum two, maximum three) advertising events for each button input. The resulting transmission sequence is shown in Figure 4 below.

CH37	CH38	CH39	Pause (20 ms)	CH37	CH38	CH39	Pause (20 ms)	CH37	CH38	CH39
------	------	------	------------------	------	------	------	------------------	------	------	------

Figure 4 – Default radio transmission sequence

3.3 User-defined radio transmission sequences

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

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

- Both commissioning telegrams and data telegrams are transmitted on the advertising channels as three advertising events. This is the default configuration and described in chapter 3.2 above.
- Commissioning telegrams are transmitted on the advertising channels as three advertising events while data telegrams are transmitted in a user-defined sequence as described below.
- Both commissioning and data telegrams are transmitted in a user-defined sequence as described below.

The selection of the transmission mode is done using the CUSTOM CHANNEL MODE register of the NFC configuration interface as described in chapter 6.7.7.

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

ExRPB supports the following user-defined sequences:

- **Three channel sequence**
This sequence is similar to the default Advertising Event with the difference that the user can select the radio channels to be used. The three channel sequence is described in chapter 3.3.1 below.
- **Two channel sequence**
In this sequence the radio telegram is transmitted using four transmissions on two radio channels. It is described in chapter 3.3.2 below.
- **One channel sequence**
In this sequence the radio telegram is transmitted using six transmissions on one radio channel. It is described in chapter 3.3.3 below.

3.3.1 Three channel sequence

The three channel radio transmission sequence is similar to the default transmission sequence. The difference is that the radio channels (BLE Channel 37, 38 and 39 in the default transmission sequence) can be selected using the Radio Channel Selection registers CH_REG1, CH_REG2 and CH_REG3.

The ExRPB advertising 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 and a transmission on the radio channel selected by CH_REG3.

This transmission sequence will be sent three times in total with pauses of 20 ms in between as shown in Figure 5 below.

CH_REG1	CH_REG2	CH_REG3	Pause (20 ms)	CH_REG1	CH_REG2	CH_REG3	Pause (20 ms)	CH_REG1	CH_REG2	CH_REG3
---------	---------	---------	------------------	---------	---------	---------	------------------	---------	---------	---------

Figure 5 – Three channel radio transmission sequence

The format of CH_REG1, CH_REG2 and CH_REG3 is described in chapter 6.7.8.

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

3.3.2 Two channel sequence

The two channel radio transmission sequence removes transmission on the third radio channel (selected by CH_REG3) and instead repeats the transmission once more (four times in total).

The ExRPB advertising 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 transmission sequence will be sent four times in total with pauses of 20 ms in between as shown in Figure 6 below.

CH_REG1	CH_REG2	Pause (20 ms)	CH_REG1	CH_REG2	Pause (20 ms)	CH_REG1	CH_REG2	Pause (20 ms)	CH_REG1	CH_REG2
---------	---------	------------------	---------	---------	------------------	---------	---------	------------------	---------	---------

Figure 6 – Two channel radio transmission sequence

The format of CH_REG1 and CH_REG2 is described in chapter 6.7.8.

3.3.3 Single channel sequence

The single channel radio transmission sequence removes transmission on the second and third radio channel (selected by CH_REG2 and CH_REG3 respectively), i.e. all transmissions will be on the radio channel selected by CH_REG1.

The ExRPB advertising telegram will be sent six times on this radio channel with pauses of 20 ms in between as shown in Figure 7 below.

CH_REG1	Pause (20 ms)	CH_REG1	Pause (20 ms)	CH_REG1	Pause (20 ms)	CH_REG1	Pause (20 ms)	CH_REG1	Pause (20 ms)	CH_REG1
---------	------------------	---------	------------------	---------	------------------	---------	------------------	---------	------------------	---------

Figure 7 – Single channel radio transmission sequence

The format of CH_REG1 is described in chapter 6.7.8.

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

4 Telegram format

ExRPB transmits radio telegrams in the 2.4 GHz band according to BLE frame structure. For detailed information about the BLE standard, please refer to the applicable specifications.

Figure 8 below summarizes the BLE frame structure.

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

Figure 8 – BLE frame structure

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

4.1 Preamble

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

4.2 Access Address

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

4.3 Header

The BLE Header identifies certain radio telegram parameters. Figure 9 below shows the structure of the BLE header.

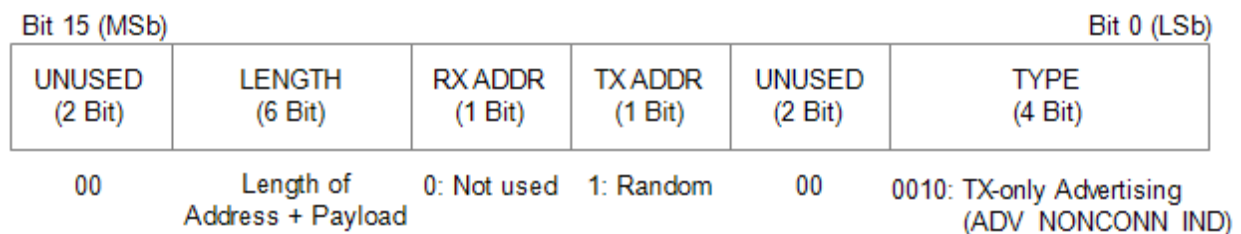


Figure 9 – BLE header structure

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

4.4 Source address

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

ExRPB supports two source address modes:

- **Static Source Address mode (default)**
In this mode, the source address is constant (but its lower 32 bit can be configured via NFC interface)
- **Private Resolvable Address mode (NFC configurable)**
In this mode, the source address changes for each transmission

ExRPB uses by default Static Source Address mode.

Private Resolvable Address mode can be selected by setting the Private Source Address flag in the Configuration register (see chapter 6.7.6) to 0b0.

These two address modes are described in the following chapters.

4.4.1 Static source address mode

By default, ExRPB uses static source addresses meaning that the source address is constant during normal operation. The static source address can be read and configured (written) via NFC as described in chapter 6.

The structure of ExRPB static addresses is as follows:

- The upper 2 bytes of the source address are used to identify the device type and set to 0xE215 for all ExRPB devices (to designate the use of an EnOcean PTM 215B module). These two bytes cannot be changed.
- The lower 4 bytes are uniquely assigned to each device. They can be changed using the NFC configuration interface as described in chapter 6.7.2

Figure 10 below illustrates the static address structure used by ExRPB.

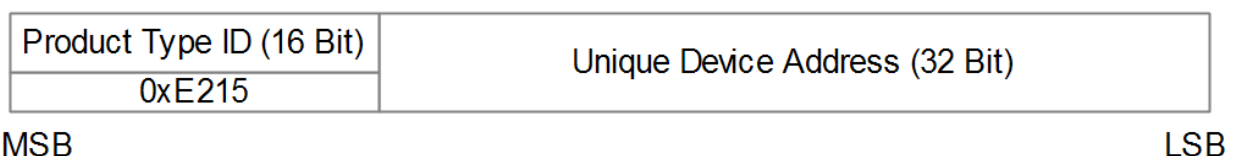


Figure 10 – BLE static source address structure

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

4.4.2 Private resolvable source address mode

For some applications it is desirable to modify (rotate) the source address used by ExRPB in order to prevent tracking of radio transmissions originating from a specific device. At the same time, each such device must remain uniquely identifiable by the receiver.

To achieve these goals, ExRPB can be configured via NFC to use random resolvable private addresses.

Using random resolvable private addresses requires that both ExRPB and the receiver both know a common key – the so-called Identity Resolution Key (IRK). ExRPB uses its device-unique random key as identity resolution key. This key can be configured via the NFC configuration interface as described in chapter 6.

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 (as described in chapter 3) 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 11 below.

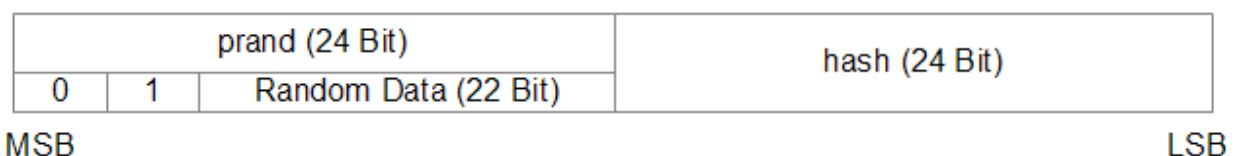


Figure 11 – BLE private resolvable source address structure

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 private resolvable source address.

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

The receiving device maintains a list of IRK for all transmitters that have been commissioned to work with it.

Whenever the receiving device receives a radio telegram with private resolvable source 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.

This mechanism is illustrated in Figure 12 below.

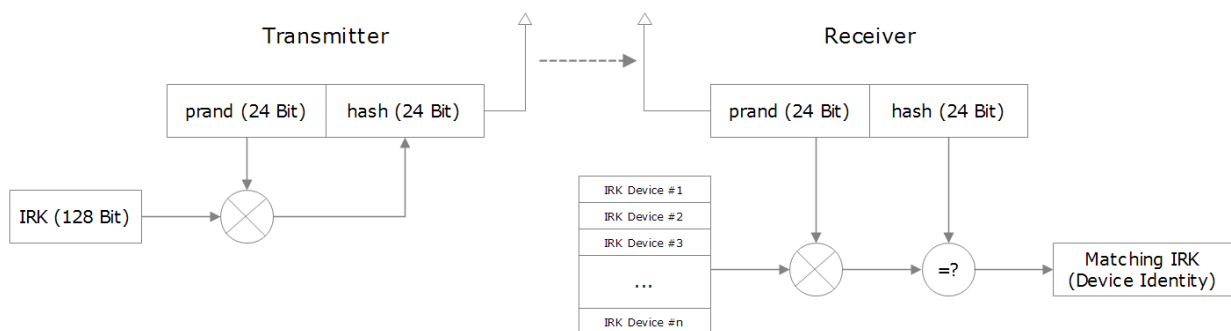


Figure 12 – Resolving private source addresses

4.5 Check Sum

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

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

4.6 Payload

The payload of data telegrams is 13 ... 17 bytes long (depending on the size of the Optional Data field) and consists of the following fields:

- **Length (1 byte)**
 The Length field specifies the combined length of the following fields. The content of the field depends on the size of the Optional Data field (which can be 0 / 1 / 2 or 4 byte).
 The resulting Length setting would be 12 / 13 / 14 or 16 byte (0x0C / 0x0D / 0x0E / 0x10) respectively
- **Type (1 byte)**
 The Type field identifies the data type used for this telegram. For PTM 215B 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. The Manufacturer ID can be changed via the NFC configuration interface as described in chapter 6.7.4.
- **Sequence Counter (4 byte)**
 The Sequence Counter is a continuously incrementing counter used for security processing. It is initialized to 0 at the time of production and incremented for each telegram (data telegram or commissioning telegram) sent.
- **Switch Status (1 byte)**
 The Switch Status field reports the button action. The encoding of this field is described in chapter 4.7.
- **Optional Data (0 / 1 / 2 or 4 byte)**
 PTM 215B provides the option to transmit additional user-defined data within each data telegram. This data can be used to identify user-specific properties.
 The length of the Optional Data field is defined in the Configuration register as described in chapter 6.7.6.
- **Security Signature (4 byte)**
 The Security Signature is used to authenticate ExRPB radio telegrams as described in chapter 4.8

Figure 13 below illustrates the data telegram payload.

0x0C ... 0x10	0xFF	Manufacturer ID 0x03DA	Sequence Counter (4 Byte)	Switch Status	Optional Data (0/1/2/4 Byte)	Security Signature (4 Byte)
LEN		TYPE				

Figure 13 – Data telegram payload structure

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

4.7 Switch status encoding

The Switch Status field within the Payload data identifies the ExRPB action (rocker push or release). ExRPB uses the following sequence to identify and transmit the rocker status:

1. Determine direction of the rocker movement (Push Action or Release Action)
2. Read input status of all button contacts
3. Calculate data payload
4. Calculate security signature

In ExRPB, the type of action (Press Action or Release Action) is indicated by Bit 0 (Energy Bar). If a button contact has been actuated during Press Action or Release Action then this is indicated by the according status bit set to '1'.

Note that all contacts that were pressed during Press Action will be released during Release Action. The case of continuing to hold one (or several) button contacts during Release Action is mechanically not possible.

The switch status encoding used by ExRPB is shown Figure 14 in below.

Switch Status							
Reserved			B1	B0	A1	A0	ACTION TYPE
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Shall be 0b000			0 = No Action 1 = Action	0 = No Action 1 = Action	0 = No Action 1 = Action	0 = No Action 1 = Action	0 = Release Action 1 = Press Action

Figure 14 – ExRPB button action encoding

In the dual rocker variant EDRPB, one rocker actuates B1 and B0 while the other rocker actuates A1 and A0.

In the single rocker variant ESRPB, the rocker actuates B1 and B0. The buttons A1 and A0 are not used.

The direction of the actuation (press or release) is indicated by the ACTION TYPE field.

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

4.8 ExRPB telegram authentication

ExRPB 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 15 below and exchanged as part of the radio telegram.

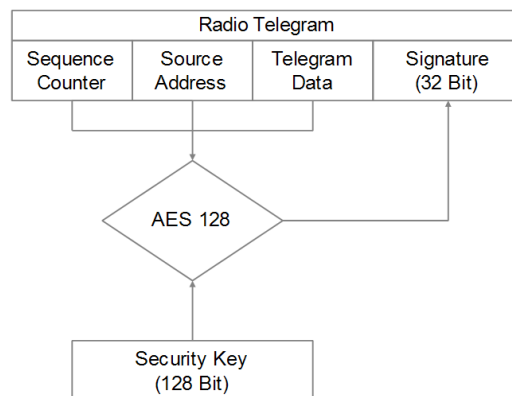


Figure 15 – Telegram authentication flow

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 ExRPB 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 (ExRPB) 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 ExRPB and only accepts messages with higher sequence counter values (i.e. not accepts equal or lower sequence counter values for subsequent telegrams).

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

4.8.1 Authentication implementation

ExRPB 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 16 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 16 – 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 17 below.

Authenticated Payload								
LEN	TYPE	MANUFACTURER	Sequence Counter				STATE	Optional Data
Byte 0	0xFF	0x03DA	Byte 0	Byte 1	Byte 2	Byte 3	Byte 0	0 / 1 / 2 / 4 byte

Figure 17 – Authenticated payload

The calculated 32 bit signature is then appended to the data telegram payload as shown in Figure 13 in chapter 4.6.

In addition to the RFC3610 standard itself, please consult also Appendix A for a step by step description of the authentication process.

5 ExRPB commissioning

Commissioning is the process by which ExRPB 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 the specific ExRPB. This is achieved by using a unique 48 Bit ID (Source Address) for each ExRPB device as described in chapter 4.4. In addition, up to 4 byte of Optional Data can be configured as described in chapter 6.7.5
- **Security parameter exchange**
The receiver needs to be able to authenticate radio telegrams from PTM 215B in order to ensure that they originate from this specific device and have not been modified as described in chapter 4.8. This is achieved by exchanging a 128 Bit random security key used by ExRPB to authenticate its radio telegrams.

ExRPB provides the following options for these tasks:

- **NFC-based commissioning**
The ExRPB parameters are read by a suitable commissioning tool (e.g. NFC smartphone with suitable software) which is already part of the network into which ExRPB will be commissioned. The commissioning tool then communicates these parameters to the intended receiver of ExRPB radio telegrams. NFC-based commissioning is described in chapter 6
- **Camera-based commissioning**
Each ExRPB module contains an optically readable Data Matrix Code (DMC) which identifies its ID and its security key. This DMC can be read by a suitable commissioning tool (e.g. smartphone) which is already part of the network into which ExRPB will be commissioned. The commissioning tool then communicates these parameters to the intended receiver of ExRPB radio telegrams. The DMC structure is described in chapter 5.2.1
- **Radio-based commissioning**
ExRPB can communicate its parameters via special radio telegrams (commissioning telegrams) to the intended receiver. To do so, ExRPB can be temporarily placed into radio-based commissioning mode as described in chapter 5.3

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

5.1 NFC-based commissioning

All required ExRPB parameters can be read via a suitable NFC reader and writer supporting the ISO/IEC 14443 Part 2 and 3 standards. The actual NFC implementation uses a Mifare Ultralight tag.

Commissioning via NFC should follow these steps:

1. Unlock ExRPB by using the default NFC PIN code `0x0000E215`
2. Read the Source Address, Security Key and Sequence Counter and configure the receiver accordingly
3. **Important:** The pre-programmed random security key used by ExRPB can be obtained both from the product DMC code as described in chapter 5.2, from received commissioning telegrams as described in chapter 5.3 and via the NFC interface. For security-critical applications where unauthorized users could have physical access to the switch it is therefore strongly recommended to change the security key to a new security key as part of the NFC-based commissioning process. To do so, follow the procedure outlined in chapter 6.7.3.
For additional security, NFC read-out of the new security key can be disabled by setting the Private Security Key flag in the Configuration register before setting the new security key.
This ensures that even persons knowing the correct PIN code to configure this specific switch cannot read out the programmed new security key. Please verify that you have properly documented the new security key as there is no possibility to retrieve this after it has been written.
4. **Important:** It is strongly recommended to disable radio-based commissioning after programming a new security key. This ensures that the new security key cannot be read out by triggering a commissioning telegram as described in chapter 5.3.
To disable radio-based commissioning, set the Disable Radio Commissioning flag in the Configuration register to `0b1`, see chapter 6.7.6.
5. **Important:** You should always change the NFC PIN code from its default setting to a new NFC PIN code and lock the NFC configuration interface. This step is mandatory to avoid access to the ExRPB configuration using the default PIN code.
Should you lose the new NFC PIN code then ExRPB can be reset to factory mode (with the default NFC PIN code) by means of a factory reset as described in chapter 5.4. For security reasons, this factory reset will always reset the security key to its pre-programmed value.

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

5.2 Camera-based commissioning via QR code

Each ExRPB contains a product label both on the product itself and on the unit packaging. The structure of this label is described in chapter 7.

As described there, this label contains a machine-readable QR (Quick Response) code of Version 5 (37 x 37 pixels, up to 122 alphanumeric characters) as shown in Figure 18 below.



Figure 18 – Example QR code

The commissioning tool can read this QR code, retrieve the necessary information (source address and security key) and send them parameters to the intended receiver of ExRPB radio telegrams.

The QR code shown in Figure 18 above encodes the following text:
30SE21501234567+Z0123456789ABCDEF0123456789ABCDEF+30PESRPB+2PDA01+S03123456

The structure of the QR code content is described below.

5.2.1 QR code format

The commissioning QR code provided by ExRPB products encodes the product parameters based on the following structure:

Data Identifier	Data Length (excluding identifier)	Data Content
30S	12 characters	Source Address: E21501234567
Z	32 characters	Security Key: 0123456789ABCDEF0123456789ABCDEF
30P	Up to 10 characters	Ordering Code: ESRPB
2P	4 characters	Step Code and Revision: DA01
S	8 characters (including leading zero)	First 2 characters: Manufacturer: 03 = Kelta Final 6 characters: Serial Number: 03123456

Table 2 – ExRPB product QR code structure

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

5.3 Radio-based commissioning

For cases where both NFC and camera-based commissioning are not feasible it is possible to set ExRPB into a specific mode where it transmits commissioning telegrams.

This functionality can be disabled via the NFC configuration interface by setting the Disable Radio Commissioning flag in the Configuration register to 0b1 (see chapter 6.7.6).

5.3.1 Commissioning mode entry

Commissioning mode is entered using a special button contact sequence. This is illustrated in Figure 19 below.

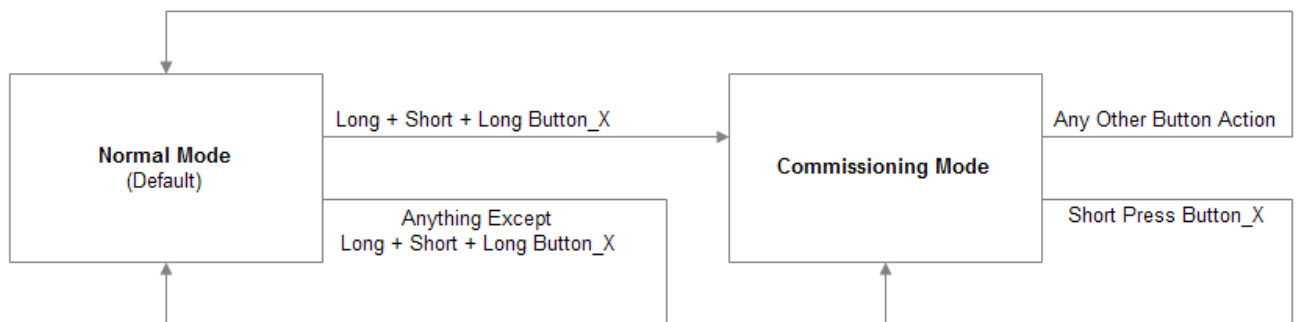


Figure 19 – Button sequence to enter radio-based commissioning mode

To enter commissioning mode, start by selecting one button (one side of one rocker) of ESRPB or EDRPB.

For the dual rocker (EDRPB) case, this button can be either upper side of left rocker, lower side of left rocker, upper side of right rocker or lower side of right rocker. For the single rocker (ESRPB) case, this can be either upper side of the rocker or lower side of the rocker. This selected button is referred to as Button_X in Figure 19 above.

Next, execute the following long-short-long sequence:

1. Press and hold the selected rocker on the selected side for more than 7 seconds before releasing it
2. Press the selected rocker on the selected side quickly (hold for less than 2 seconds)
3. Press and hold the selected rocker on the selected side again for more than 7 seconds before releasing it

Upon detection of this sequence, ExRPB will enter commissioning mode if the Disable Radio Commissioning flag in the Configuration register of the NFC interface is set to 0b0 (default state).

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

5.3.2 Commissioning telegram transmission

ExRPB will transmit a commissioning telegram (on the radio channels selected as described in chapter 3.1) upon entering commissioning mode.

ExRPB will continue to transmit commissioning telegrams whenever the button used for entry into commissioning mode (Button_X) is pressed or released again.

The payload of commissioning telegrams is 30 bytes long and consists of the following fields:

- **Length (1 byte)**
The Length field specifies the combined length of the following fields. For ExRPB commissioning telegrams, this field is always set to 0x1D to indicate 29 byte of manufacturer-specific data
- **Type (1 byte)**
The Type field identifies the data type used for this telegram. This field is set to 0xFF to indicate a "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. By default, this field is set to 0x03DA (EnOcean GmbH). This field can be changed via the NFC configuration interface as described in chapter 6.7.4.
- **Sequence Counter (4 byte)**
The Sequence Counter is a continuously incrementing counter used for security processing. It is initialized to 0 at the time of production and incremented for each telegram (data telegram or commissioning telegram) sent.
- **Security Key (16 byte)**
Each PTM 215B module contains its own 16 byte device-unique random security key which is generated and programmed during manufacturing. It is transmitted during commissioning to enable the receiver to authenticate PTM 215B data telegrams
- **Static Source Address (6 byte)**
The Static Source Address is used to uniquely identify each BLE device. It is transmitted as part of the BLE frame as described in chapter 4.4.1. Some devices (most notable all iOS-based products) however do not expose this address to their applications. This makes it impossible to use such applications to commission ExRPB. The Static Source Address is therefore again transmitted as part of the payload.

Figure 20 below illustrates the commissioning telegram payload.

LEN	TYP	Manufacturer ID	Manufacturer-specific Data		
			Sequence Counter (4 Byte)	Security Key (16 Byte)	Static Source Address (6 Byte)
0x1D	0xFF	0x03DA			

Figure 20 – Commissioning telegram payload structure

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

5.3.3 Exit from commissioning mode

Pressing any key except the button used for entry into commissioning mode (Button_X) will cause ExRPB to stop transmitting commissioning telegrams and return to normal data telegram transmission.

5.4 Factory Reset

ExRPB can be reset to its default settings by means of a factory reset.

This ensures that ExRPB can be reset to a known configuration in case the PIN for the NFC access has been lost or NFC access is not possible for other reasons

In order to execute such factory reset, the rocker(s) and the switch housing have to be removed from ExRPB so that all four ExRPB module contacts and the energy bar are accessible.

After that, all four button contacts (A0, A1, B0 and B1) have to be pressed at the same time while the energy bow of the ExRPB module is pressed down.

The energy bow must then be held at the down position for at least 10 seconds before being released. The button contacts A0, A1, B0 and B1 can be released at any time after pressing the energy bow down, i.e. it is no requirement to hold them as well for at least 10 seconds.

Upon detecting this input, ExRPB will restore the default settings of the following items:

- Static Source Address
- Security Key and Security Key Write register
Both registers will be restored to the value of the factory-programmed security key
- Manufacturer ID
The manufacturer ID will be reset to 0x03DA (EnOcean GmbH)
- NFC PIN Code
The NFC PIN Code will be reset to 0x0000E215

After such factory reset, Source Address and Security Key will again match the content of the DMC code on the unit label as described in chapter 7.

In addition, ExRPB will reset the following registers:

- Configuration register (to 0x00)
- Custom Channels Register (to 0x00)

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

6 NFC interface

ExRPB implements NFC Forum Type 2 Tag functionality as specified in the ISO/IEC 14443 Part 2 and 3 standards using an NXP NT3H2111 Mifare Ultralight tag.

This NFC functionality can be used to access (read and write) the ExRPB configuration memory and thereby configure the device as described in the following chapters.

Chapter 6.1 below gives an introduction to the NFC functionality and options to use the NFC interface.

For in-depth support for integrating the NXP NT3H2111 NFC functionality into PC or smartphone SW please contact NXP technical support.

6.1 Using the NFC interface

Using the NFC interface requires the following:

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

EnOcean recommends TWN4 from Elatec RFID Systems (<https://www.elatec-rfid.com/en/>) as USB NFC reader. This reader is shown in Figure 21 below.



Figure 21 – Elatec TWN4 MultiTech Desktop NFC Reader

TWN4 can be configured as CDC / Virtual COM port and can then be accessed like any serial interface. It provides all necessary commands for the NFC interface, specifically to:

- Read data from configuration memory and write data to configuration memory
- Authenticate the user (to allow read / write of protected memory) via 32 bit PIN

NFC functionality is also available in certain Android smartphones and tablets. NXP provides a SW framework that can be used with Android devices and can advise regarding suitable tablets and smartphones.

NFC communication distance is for security reasons set to require direct contact between reader and switches based on ExRPB.

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

6.2 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.

6.2.1 NFC interface state machine

Figure 22 below shows the overall state machine of the NFC interface.

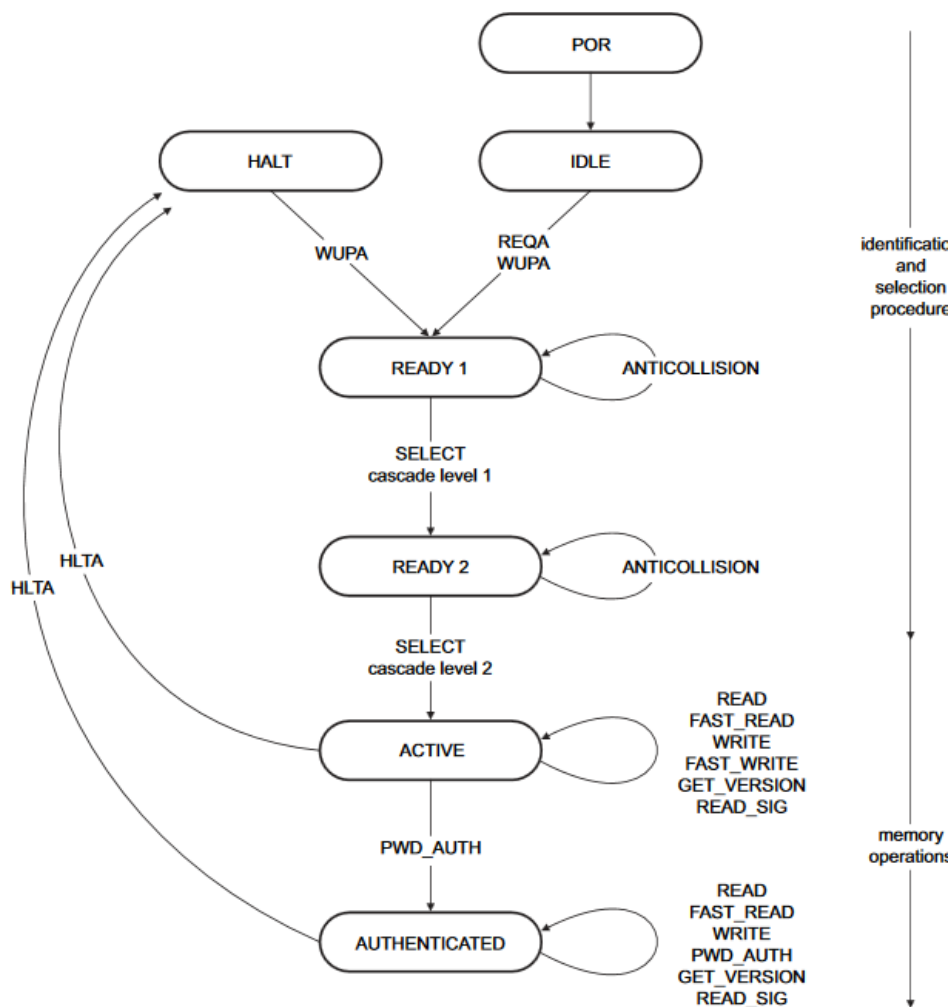


Figure 22 – NFC interface state machine

6.2.2 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.

6.2.3 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.

6.2.4 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.

6.2.5 ACTIVE state

ACTIVE state enables read and write accesses to unprotected memory.

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

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

6.2.6 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 23 below shows the read command sequence.

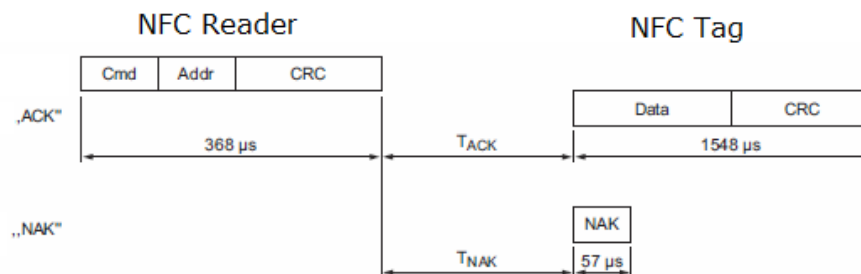


Figure 23 – NFC read command sequence

6.2.7 Write command

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

Figure 24 below shows the read command sequence.

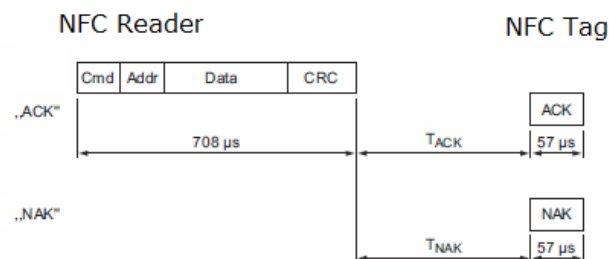


Figure 24 – NFC write command sequence

6.2.8 Password authentication (PWD_AUTH) command

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

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

Figure 25 below shows the password authentication sequence.

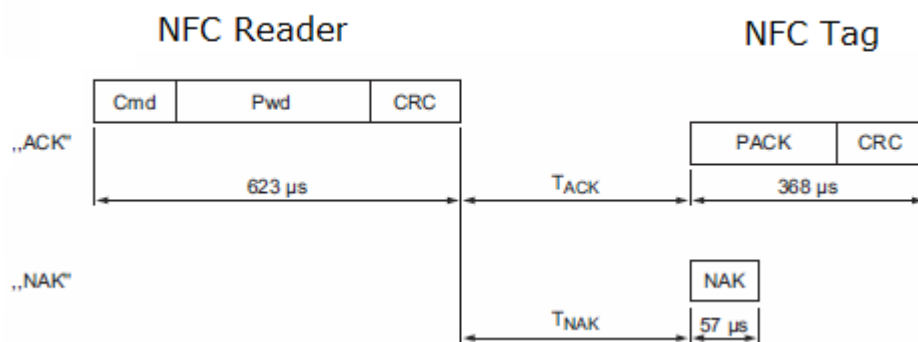


Figure 25 – Password authentication sequence

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

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

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

6.3 Using TWN4 as USB NFC reader

Elatec RFID Systems provides a PC software called "Director" as part of their software support package. At the time of writing, this was available from this address:

<https://www.elatec-rfid.com/en/download-center/contact-form-twn4-devpack-sdk/>

Figure 26 below shows the user interface of this software.

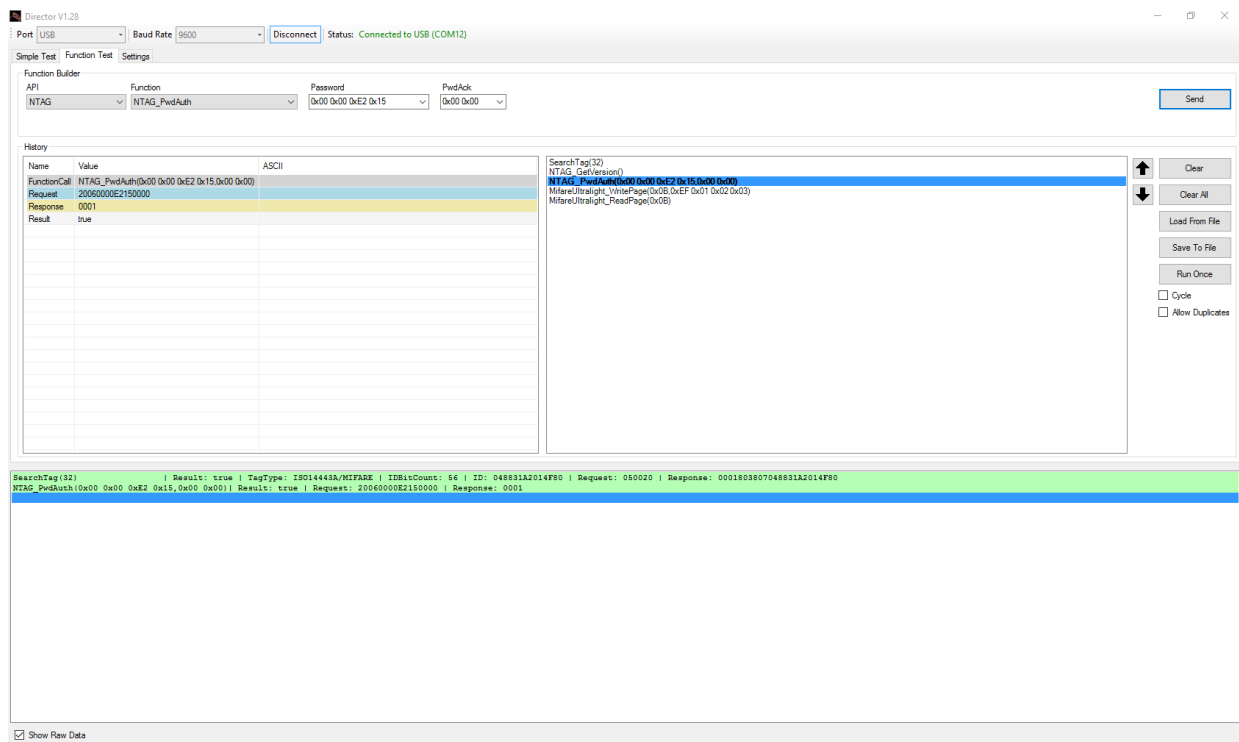


Figure 26 – User interface of TWN4 Director

By using this software, it is easily possible to generate the required serial commands that have to be sent via CDC / Virtual COM port to TWN4 and understand the structure of the response that will be received back.

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

6.3.1 Useful commands

The following commands are especially useful:

- **SearchTag(maximum ID bytes)**
Used to search for a connected tag and identify type and ID of such tag. This should always be used as first operation ahead of any read / write / authenticate actions.
Example: SearchTag(32)
- **NTAG_PwdAuth(32 bit password as hex bytes, 16 bit password_ack as hex bytes)**
Used to authenticate access to the protected memory area
Example: NTAG_PwdAuth(0x00 0x00 0xE2 0x15, 0x00 0x00)
- **NTAG_Read(page)**
Used to read one page of data
Example: NTAG_Read(0x04)
- **NTAG_Write(page, data)**
Used to write one page of data
Example: NTAG_Write(0x40, 0x12 0x34 0x56 0x78)
- **NTAG_Write(0xE5, PIN Code)**
Used to set a new pin code by writing to page 0xE5
Example: NTAG_Write(0xE5, 0x12 0x34 0x56 0x78)

6.3.2 Translation into binary data

In order to use these commands within a user application, they have to be translated into raw data. This can be done by enabling the "Show Raw Data" feature in the command log of the Director software as shown in Figure 27 below.

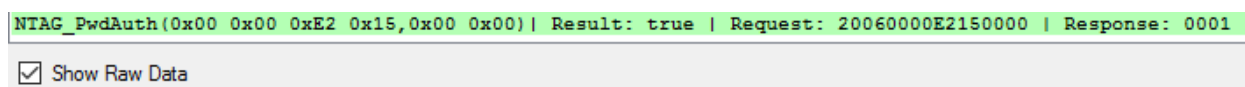


Figure 27 – Enabling raw data display

This raw data can then be transmitted to TWN4 via a virtual COM port. TWN4 will respond to the request with the corresponding response as shown in Figure 28 below.



Figure 28 – Binary data exchange

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

6.4 Configuration memory organization

The ExRPB configuration memory is divided into the following areas:

- Public data
- Protected data

In addition to that, ExRPB maintains a private configuration memory region used to store default parameters and confidential information which is not accessible to the user.

Figure 29 below illustrates the configuration memory organization used by ExRPB.

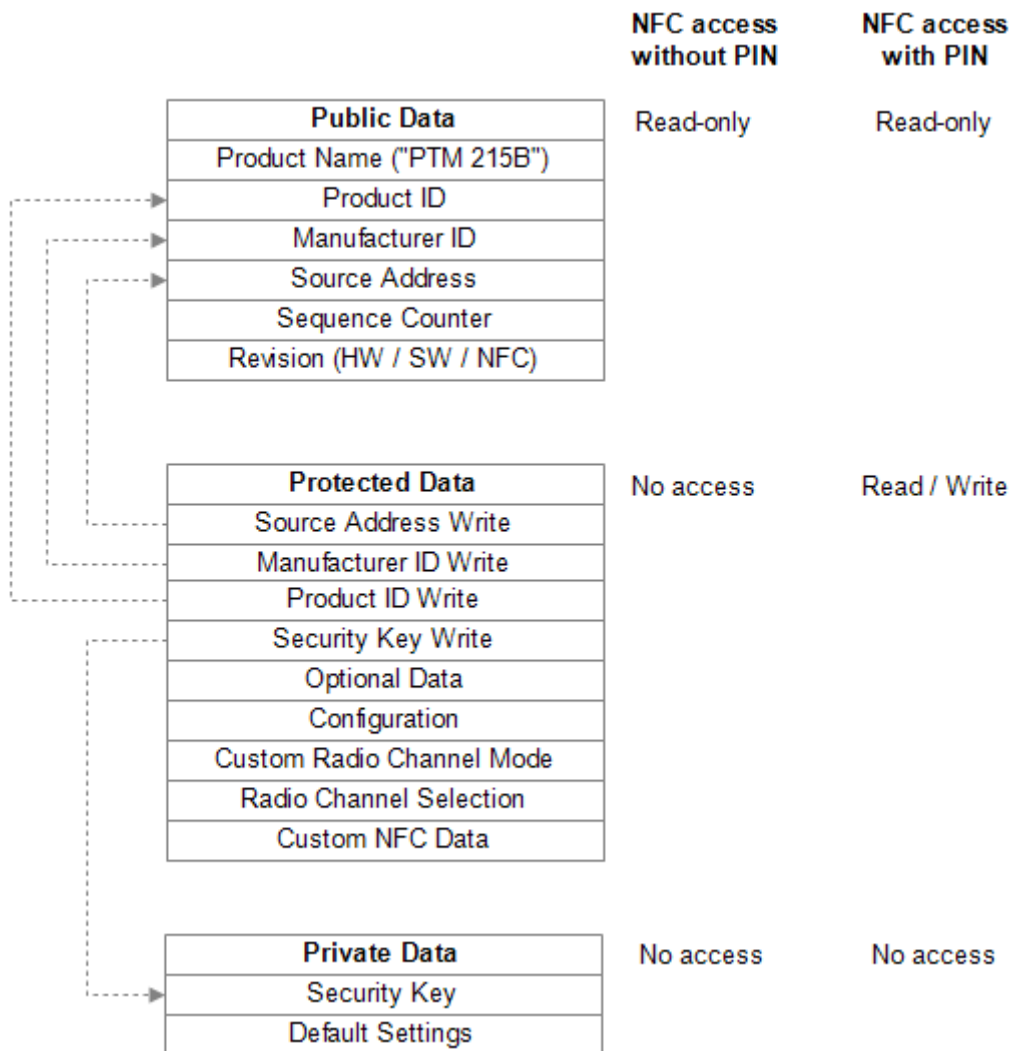


Figure 29 – Configuration memory organization

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD
6.5 Memory Address Map

The NFC-accessible configuration memory is organized in memory pages where each memory page is 4 byte wide. An NFC access reads 16 bytes (4 pages) or writes 4 bytes (one page). The addresses map of the configuration memory is shown in Table 3 below. The byte order is little endian, i.e. byte 0 will be read first and byte 3 last.

Area	NFC Page	Byte Offset	Byte 0 (LSB)	Byte 1	Byte 2	Byte 3 (MSB)
Public Memory Area						
Public	0 (0x00)	0	Reserved			
Public				
Public	3 (0x03)	12				
Public	4 (0x04)	16	Product Name "PTM 215B"			
Public	5 (0x05)	20				
Public	6 (0x06)	24	Product ID			
Public	7 (0x07)	28				
Public	8 (0x08)	32	NFC Revision		Manufacturer ID	
Public	9 (0x09)	36	Reserved			
Public	10 (0x0A)	40	Hardware Revision			
Public	11 (0x0B)	44	Software Revision			
Public	12 (0x0C)	48	Static Source Address			
Public	13 (0x0D)	52	Sequence Counter			
Protected Memory Area						
Protected	14 (0x0E)	56	Configuration	Custom CH Mode	Reserved	
Protected	15 (0x0F)	60	Opt Data 0	Opt Data 1	Opt Data 2	Opt Data 3
Protected	16 (0x10)	64	Product ID Write			
Protected	17 (0x11)	68				
Protected	18 (0x12)	72	Source ID Write			
Protected	19 (0x13)	76	Manufacturer ID Write		Reserved	
Protected	20 (0x14)	80	Security Key Write			
Protected				
Protected	23 (0x17)	92				
Protected	24 (0x18)	96	CH_REG1	CH_REG2	CH_REG3	Reserved
Protected	25 (0x19)	100	Reserved			
Protected				
Protected	31 (0x1F)	124				
Protected	32 (0x20)	128	Customer NFC Data			
Protected				
Protected	95 (0x5F)	380				
Protected	96 (0x60)	384	Reserved			
Protected				
Protected	225 (0x10)	900				
Protected	229 (0xE5)	916	PIN Code (Write Only)			

Table 3 – Configuration memory address map

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

6.6 Public data

Public data can be read by any NFC-capable device supporting the ISO/IEC 14443 Part 2 and 3 standards. No specific security measures are used to restrict read access to this data.

The following items are located in the public data area:

- **Product Name**
This is always "PTM 215B" to designate the PTM 215B module used within the EDRPB or ESRPB rocker switch
- **Product ID**
This is an 8 byte field which is by default set to 0x0000000000000000.
Product ID and Manufacturer ID can be configured by the customer as required to uniquely identify his products, see chapter 6.7.4
- **Manufacturer ID**
This is an 2 byte field used to identify the manufacturer of a BLE product, see chapter 4.6. This field is by default set to 0x03DA (EnOcean GmbH).
Product ID and Manufacturer ID can be configured by the customer as required to identify his products, see chapter 6.7.4
- **Static Source Address**
This is a 4 byte field used to identify the static source address used by ExRPB, see chapter 4.4.1. Each ExRPB is pre-programmed with an individual static source address.
The Static Source Address can be configured by the customer as required to identify his product, see chapter 6.7.2
- **Hardware Revision, Software Revision and NFC Revision**
These fields identify the device revision
- **Telegram sequence counter**
This is a 4 byte field which is initialized to 0 during manufacturing and incremented for each transmitted telegram. Receivers shall never accept telegrams containing sequence counter values equal or less than previously received values to avoid replay attacks.

Changing the Static Source Address, Manufacturer ID and Product ID fields is only possible via protected data access as described below to prevent unauthorized modification.

For security reasons, the telegram sequence counter cannot be written or reset by any mechanism.

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

6.7 Protected Data

The following items are located in the protected data area:

- **Source Address Write register**
This 4 byte register is used to update the lower 4 byte of the Static Source Address, see chapter 6.7.2
- **Product ID Write register**
This 8 byte register is used to update the Product ID, see chapter 6.7.4
- **Manufacturer ID Write register**
This 4 byte register is used to update the Manufacturer ID, see chapter 6.7.4
- **Security Key Write register**
This 16 byte register is used to update the security key used by ExRPB, see chapter 6.7.3
- **Optional Data register**
This 4 byte register contains optional data that can be transmitted as part of all data telegrams, see chapter 4.6. Optional Data 0 is sent first, Optional Data 3 last.
- **Configuration register**
This 1 byte register is used to configure the functional behavior of ExRPB, see chapter 6.7.6
- **Custom Channel Mode register**
This 1 byte register is used to configure the number of different radio channels used for data and commissioning telegram transmission, see chapter 6.7.7
- **Radio Channel Selection registers (CH_REG1, CH_REG2 and CH_REG3)**
These 1 byte registers are used to configure the actual radio channels used whenever the Custom Channel Mode register is set to a user-defined value, see chapter 6.7.8
- **Custom NFC Data**
ExRPB reserves 64 byte for customer-specific NFC data, see chapter 6.7.9

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

6.7.1 PIN Code

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 0x0000E215.

The default pin code shall be changed to a user-defined value as part of the installation process. This can be done by unlocking the NFC interface with the old PIN code and then writing the new PIN code to page 0xE5 as described in chapter 6.3.1.

6.7.1 Configuration of product parameters

PTM 215B allows no direct modification of the following parameters:

- Static Source Address
- Product ID
- Manufacturer ID
- Security Key

In order to modify these parameters, the user has to write the new value into specific registers (Source Address Write, Product ID Write, Manufacturer ID Write and Security Key Write) in the protected data area and set the according Update flag in the Configuration register.

After that, the user has to push and release one rocker of ESRPB or EDRPB.

6.7.2 Source Address Write register

The Source Address Write register is 4 byte wide and can be used to modify the lower 32 bit of the Static Source Address. The upper 16 bit of the Static Source Address are always fixed to 0xE215 to identify the module type (PTM 215B).

In order to do change the lower 32 bit of the Static Source Address, follow these steps:

1. Write new source address into the Source Address Write register
2. Set the Update Source Address flag in the Configuration register to 0b1
3. Actuate (press and release) one rocker of ESRPB / EDRPB

ExRPB will determine that it should modify the Static Source Address based on the setting of the Update Source Address flag and copy the value of the Source Address Write register to the lower 32 bit of the Source Address register.

After successful execution, ExRPB will clear the Update Source Address flag to 0b0.

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

6.7.3 Security Key Write register

The Security Key Write register is 16 byte wide and contains the device-unique random security key.

The factory programmed key can be replaced with a user defined key by following these steps:

1. Write new security key into the Security Key Write register
Note that for security reasons, setting the Security Key to the following values is not possible:
 - 0x00000000000000000000000000000000
 - 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFIf the Security Key Write register is set to one of these values then no update of the Security Key will occur.
2. Set the Update Security Key flag in the Configuration register to 0b1
3. If the key should be write-only (not readable after the key update) then set the Private Security Key flag in the Configuration register to 0b1
4. Actuate (press and release) one rocker of ESRPB / EDRPB

ExRPB will determine that it should modify the security key based on the setting of the Update Security Key flag and copy the value of the Security Key Write register to the Security Key register in private memory.

After successful execution, ExRPB will clear the Update Security Key flag to 0b0.

If the Private Key flag in the Configuration register is set to 0b0 then the content of the Security Key Write register will be maintained at its current value. This addresses use cases where the security key shall be readable for users having the correct PIN code.

If the Private Key flag in the Configuration register is set to 0b1 then the content of the Security Key Write register will be cleared to 0x00000000000000000000000000000000 after successful execution. This addresses use cases where the security key shall never be readable (even for users having the correct PIN code).

The Security Key Write register will maintain this value of 0x00000000000000000000000000000000 even if the Private Key flag in the Configuration register is subsequently cleared to 0b0. This ensures that it is not possible to read a security key which was written with the Private Key flag in the Configuration register being set.

Note that it is not possible to read the current security key via NFC if the Security Key Write register has been accidentally overwritten or cleared via NFC write. In this case it is necessary to write a new security key (as described above) or to reset the device to its default security key by means of a factory reset.

The protected memory is designed to support 1000 modifications of the security key.

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

6.7.4 Product ID and Manufacturer ID Write register

The Product ID register is 8 byte wide and can be used to specify a publicly-accessible parameter (e.g. a user-specific ID or name) that can be read by an NFC commissioning tool in order to determine the specific product type.

The Manufacturer ID is 2 byte wide and specifies the manufacturer of a BLE product and is transmitted as part of each BLE telegram. By default, the manufacturer ID is set to 0x03DA (EnOcean GmbH) but it can be changed to a different OEM identifier.

Product ID and Manufacturer ID can be changed by following these steps:

1. Write the desired Product ID (8 byte using HEX or ASCII encoding according to user choice) into the Product ID Write register. Setting the Product ID register to 0x0000000000000000 will cause ExRPB not to update the Product ID.
2. Write the desired Manufacturer ID (2 byte) into the Manufacturer ID Write register. Setting the Manufacturer ID Write register to 0x0000 will cause ExRPB not to update the Manufacturer ID.
3. Set the Update Product and Manufacturer ID flag in the Configuration register to 0b1
4. Actuate (press and release) one rocker of ESRPB / EDRPB

ExRPB will determine that it should update the Product ID and Manufacturer ID based on the setting of the Update Product and Manufacturer ID flag and copy any non-zero value of the Product ID Write register to the Product ID register and any non-zero value of the Manufacturer ID Write Register to the Manufacturer ID register.

After that, ExRPB will clear the Update Product and Manufacturer ID flag to 0b0.

6.7.5 Optional Data register

The Optional Data register can be used to specify up to 4 byte of custom data that will be transmitted as part of each data telegram. This optional data can store user-specific or application-specific information.

The size of the Optional Data field is specified in the Configuration register and can be 0 byte (not present, default), 1 byte, 2 byte or 4 byte.

If the size of the Optional Data field is set to a non-zero value in the Configuration register then ExRPB will read the corresponding amount of data from the Optional Data register beginning with the least significant byte (Byte 0 – Optional Data 0).

Note that using the optional data feature requires additional energy for the radio telegram transmission and might therefore reduce the total number of redundant telegrams which are transmitted.

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

6.7.6 Configuration register

The Configuration register is 1 byte wide and contains configuration flags. Figure 30 below shows the structure of the Configuration register.

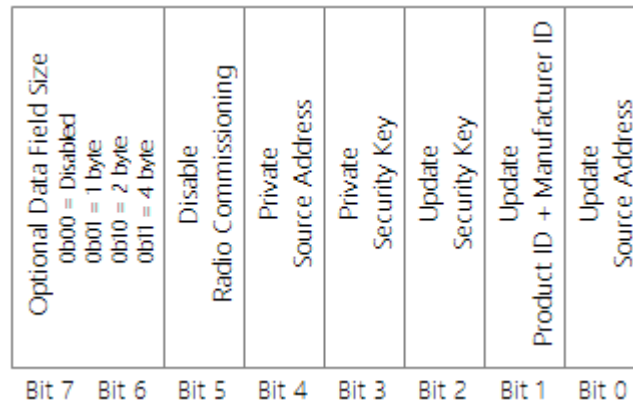


Figure 30 – Configuration register structure

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

6.7.7 Custom Channel Mode register

The Custom Channel Mode register is 1 byte wide and allows selection of the custom radio transmission modes as described in chapter 3.3.

Table 4 below shows the supported custom radio transmission settings.

Setting	Meaning
0x00 (Default)	Commissioning and data telegrams in standard Advertising Mode (Using BLE Advertising Channels CH37, CH38 and CH39) Note: This is equivalent to setting Custom Channel Mode = 0x04 in conjunction with CH_REG1 = 0x25, CH_REG2 = 0x26 and CH_REG3 = 0x27
0x01	Commissioning telegrams in standard Advertising Mode Data telegrams on 3 user-defined radio channels
0x02	Commissioning telegrams in standard Advertising Mode Data telegrams on 2 user-defined radio channels
0x03	Commissioning telegrams in standard Advertising Mode Data telegrams on 1 user-defined radio channel
0x04	Commissioning and Data telegrams on 3 user-defined radio channels
0x05	Commissioning and Data telegrams on 2 user-defined radio channels
0x06	Commissioning and Data telegrams on 1 user-defined radio channel
0x07 ... 0xFF	Unused, will be treated as 0x00

Table 4 – Custom Channel Mode register settings

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

6.7.8 Radio Channel Selection registers

If the Custom Channel Mode register is set to a value other than 0x00 then the radio channels for transmission are selected using the CH_REG1, CH_REG2 and CH_REG3 registers as described in chapter 3.3. Each of these registers is 1 byte wide and uses the encoding shown in Table 5 below.

Note that two channel types can be used:

- Standard BLE radio channels (BLE Channel 0 ... BLE Channel 39 using the even frequencies from 2402 MHz to 2480 MHz as described in chapter 3)
- Custom radio channels in between the standard BLE channels (odd frequencies from 2403 MHz to 2479 MHz)

CH_REGn Value	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 5 – Radio Channel Selection register settings

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

6.7.9 Customer Data

ExRPB allocates 64 pages (256 byte) for customer data that can be read and written via the NFC interface in protected mode.

The main intention is to enable storing OEM-specific information such as product type, revision, date code or similar. There is however no restriction (other than the maximum size of 256 byte) on the type of content that can be stored in this memory region.

ExRPB will not access or modify this memory region.

Users should keep in mind that the content of this memory region will not be affected by a factory reset. This means that after a factory reset, the content of this memory region can be read using the default PIN code. This region should therefore not be used to store sensitive data.

6.8 Private Data

The private data area stores the following items:

- Security Key
- Default settings

The content of the private data area is not externally accessible.

6.8.1 Security Key

The Security Key field contains the 128 bit private key used for authenticating ExRPB telegrams and for resolving private source addresses.

This register is programmed with a random value during manufacturing. It can be changed using the Security Key Write feature described in chapter 6.7.3.

6.8.2 Default Settings

The Default Settings field contains a backup of the following PTM 215B factory settings:

- Static Source Address
- Security Key
- Manufacturer ID
- NFC PIN Code

These default settings can be restored by means of a factory reset as described in chapter 5.4.

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

7 Device Label

Each ESRPB or EDRPB rocker pad contains a product label as shown in Figure 31 below.



Figure 31 – ESRPB / EDRPB product label

This device label identifies the following parameters:

- (1) Frequency and radio standard (2.4 GHz BLE in above example)
- (2) Product revision (DA-01 in above example)
- (3) Manufacturing date (week 35, 2016 in above example)
- (4) QR code for automated reading of all information (see chapter 5.2.1.)
- (5) Static Source Address (E21501234567 in above example)
- (6) Manufacturer and Serial Number (03123456 in above example)

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

8 APPLICATION INFORMATION

8.1 Transmission range

The main factors that influence the system transmission range are:

- Type and location of the antennas of receiver and transmitter
- Type of terrain and degree of obstruction of the link path
- Sources of interference affecting the receiver
- "Dead spots" caused by signal reflections from nearby conductive objects.

Since the expected transmission range strongly depends on this system conditions, range tests should always be performed to determine the reliably achievable range under the given conditions.

The following figures should be treated as a rough guide only:

- Line-of-sight connections
Typically 10 m range in corridors, up to 30 m in halls
- Plasterboard walls / dry wood
Typically 10 m range, through max. 2 walls
- Ferro concrete walls / ceilings
Typically 5 m range, through max. 1 ceiling (depending on thickness)
- Fire-safety walls, elevator shafts, staircases and similar areas should be considered as shielded

The angle at which the transmitted signal hits the wall is very important. The effective wall thickness – and with it the signal attenuation – varies according to this angle. Signals should be transmitted as directly as possible through the wall. Wall niches should be avoided.

Other factors restricting transmission range include:

- Switch mounting on metal surfaces (up to 30% loss of transmission range)
- Hollow lightweight walls filled with insulating wool on metal foil
- False ceilings with panels of metal or carbon fibre
- Lead glass or glass with metal coating, steel furniture

The distance between the receiver and other transmitting devices such as computers, audio and video equipment that also emit high-frequency signals should be at least 0.5 m.

8.2 External magnets

ExRPB is powered by an electromagnetic harvester. Using magnets (e.g. for mounting) in close proximity to ExRPB therefore has to be avoided.

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

8.3 Receiver configuration

ExRPB communicates user actions (rocker push / release) using a sequence of advertising telegrams as described in chapter 3.

In order to maximize the likelihood of reception of these telegrams, it is necessary that the receiver is either permanently in receive mode on the selected radio channels or – if this is not possible – is in receive mode periodically on one of the chosen radio channels for a certain minimum period of time.

The two key timing parameters for the periodical reception case are the scan interval (time between the start of two consecutive scanning cycles) and the scan duration (for how long will the receiver scan within each scanning cycle).

ExRPB transmits the advertising events with a pause interval of 20 ms between two transmissions. The transmission of the advertising event itself requires approximately 1 ms per radio channel (meaning approximately 3 ms in total when using 3 radio channels) which means that the total time between the start of two advertising events is approximately 23 ms.

Considering that the receiver might start scanning directly after the start of one transmission, we can therefore determine that it should remain active (scan duration) for at least 23 ms to check for the start of the next transmission.

Likewise, we need to ensure that the receiver will become active (scan period) no later than right before the beginning of the third advertising event. So the longest period for which the receiver can be inactive is given by the time from the beginning of the first advertising events until the beginning of the third advertising event, meaning approximately 46 ms in total.

The likelihood of correct reception obviously increases if more than one of the redundant advertising events is received. It should also be considered that the receiver is typically scanning on different radio channels. Therefore the theoretical maximum of 46 ms should be significantly reduced to increase the likelihood of correct reception.

It is therefore recommended to use a setting of 30 ms scan period and 23 ms scan interval for cases where continuous reception is not possible.

9 REGULATORY INFORMATION

The PTM 215B module within ESRPB and EDRPB has been certified according to FCC, IC and CE regulations. Changes or modifications not expressly approved by EnOcean could void the user's authority to operate the equipment.

9.1 CE / RE-D for Europe Union

The Radio Equipment Directive (2014/53/EU, typically referred to as RED) has replaced the old R&TTE directive from 1999 as regulatory framework for radio products in the European Union. All products sold to final customers after 12th of June, 2017 have to be compliant to RED.

At the time of writing, the text of the RED legislation was available from this link:
<http://eur-lex.europa.eu/eli/dir/2014/53/oj>

It is the responsibility of the OEM manufacturer to demonstrate compliance to all applicable EU directives and standards. The attestation of conformity for PTM 215B serves as input to the declaration of conformity for the full product.

At the time of writing, guidance on the implementation of EU product rules – the so called “Blue Guide” – was available from this link:
<http://ec.europa.eu/DocsRoom/documents/18027/>

Specifically within the new RED framework, all OEM manufacturers have for instance to fulfill the following additional requirements:

- Provide product branding (on the product) clearly identifying company name or brand and product name as well as type, charge or serial number for market surveillance
- Include (with the product) documentation containing full postal address of the manufacturer as well as radio frequency band and max. transmitting power
- Include (with the product) user manual, safety information and a declaration of conformity for the final product in local language
- Provide product development and test documentation upon request

Please contact an accredited test house for detailed guidance.

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

9.2 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: 09/26/2016

Application Dated: 09/26/2016

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-PTM215B
Name of Grantee: EnOcean GmbH
Equipment Class: Part 15 Low Power Communication Device
Transmitter
Notes: 2402 MHz - 2480 MHz transmitter

Grant Notes

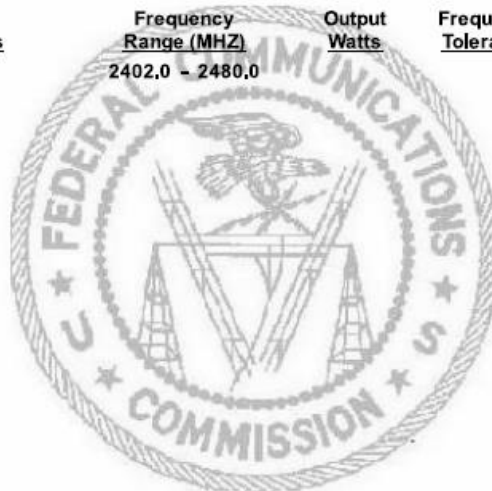
FCC Rule Parts
15C

Frequency
Range (MHZ)
2402,0 - 2480,0

Output
Watts

Frequency
Tolerance

Emission
Designator



9.2.1 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.

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

9.3 IC (Industry Canada) Certificate



FCB under the Canada-EC MRA
TCB under the USA-EC MRA
RFCAB under the Japan-EC MRA
Notified Body R&TTE Directive 99/5/EC
Notified Body RED Directive 2014/53/EU
Notified Body EMC Directive 2014/30/EU
No. CA001711G

TECHNICAL ACCEPTANCE CERTIFICATE CANADA

CERTIFICAT D'ACCEPTABILITÉ TECHNIQUE CANADA

CERTIFICATION No. 5713A-PTM215B
No. DE CERTIFICATION
ISSUED TO EnOcean GmbH
DELIVRE A

Street Address Kolpingring 18 a
Numéro et rue
Province or State Germany
Province ou Etat

TYPE OF EQUIPMENT Low Power Device (2400–2483.5 MHz)
GENRE DE MATERIEL

ANTENNA Integrated
ANTENNE Incorporé

ANTENNA GAIN
GAIN D'ANTENNE

City Oberhaching
Ville
Postal Code 82041
Code postal

PMN PTM 215B
HVIN PTM 215B
FVIN

FREQUENCY RANGE BANDE DE FRÉQUENCES	EMISSION TYPE GENRE D'ÉMISSION	RF POWER PUISSANCE H.F.	SPECIFICATION / ISSUE / DATE SPÉCIFICATION / ÉDITION / DATE
2402 - 2480 MHz	947KG1D	96.6 dBµV/m	RSS-210 / 9 / August 2016

TEST LABORATORY EMCCons DR. RASEK GmbH & Co. KG
LABORATOIRE D'ESSAY

Street Address Stoernhofer Berg 15
Numéro et rue
Province or State Germany
Province ou Etat

Name Ludwig Kraft
Nom
E-mail lkraft@emcc.de

CN 3464C OATS 3464C-1
City Unterleinleiter
Ville
Postal Code 91364
Code Postal
Tel +49 9194 7263-301
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 ISDE 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 ISDE. 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 ISDE.

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 l'espécification ci-dessus.

DATE 26 September 2016

Certification Officer

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

9.3.1 IC (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."

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

9.4 ACMA (Australia) Declaration of Conformity

Supplier's Declaration of Conformity



As required by the following Notices:

- > *Radiocommunications (Compliance Labelling - Devices) Notice 2014* made under section 182 of the *Radiocommunications Act 1992*;
- > *Radiocommunications Labelling (Electromagnetic Compatibility) Notice 2008* made under section 182 of the *Radiocommunications Act 1992*
- > *Radiocommunications (Compliance Labelling – Electromagnetic Radiation) Notice 2014* made under section 182 of the *Radiocommunications Act 1992* and
- > *Telecommunications (Labelling Notice for Customer Equipment and Customer Cabling) Instrument 2015* made under section 407 of the *Telecommunications Act 1997*.

Instructions for completion

- > **Do not return this form to the ACMA.** This completed form must be retained by the supplier as part of the documentation required for the compliance records and must be made available for inspection by the ACMA when requested.

Supplier's details (manufacturer, importer or authorised agent)

Company Name (OR INDIVIDUAL)

ACN/ABN

Compliance Folder Management Pty Ltd

ABN 75 082 447 194

On behalf of: EnOcean GmbH



Street Address (AUSTRALIAN)

Unit 1, 570 City Road

South Melbourne

Victoria, 3205

Product details and date of manufacture

Product description – brand name, type, current model, lot, batch or serial number (if available), software/firmware version (if applicable)

Brand:	Dolphin
Model:	PTM 215B
Description:	Bluetooth (LE) Pushbutton Transmitter Module
Manufacturer:	EnOcean GmbH Kolpingring 18a, 82041 Oberhaching, Germany
Date of manufacture or importation of the original/modified item	

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

Compliance – applicable standards and other supporting documents

Evidence of compliance with applicable standards may be demonstrated by test reports, endorsed/accredited test reports, certification/competent body statements.

Having had regard to these documents, I am satisfied the above mentioned product complies with the requirements of the relevant ACMA Standards made under the *Radiocommunications Act 1992* and the *Telecommunications Act 1997*.

List the details of the documents the above statement was made, including the standard title, number and, if applicable, number of the test report/endorsed test report or certification/competent body statement

Radiocommunications (Short Range Devices) Standard 2014 (Amnt 1 : 2015)
Radiocommunications (Low Interference Potential Devices) Class Licence 2015
AS/NZS 4288: 2017
WLAN 2.4GHz :
EN 300 328 V1.9.1
Bluetooth (LE) - Report No.: 16/06-0033, Dated: 18 August 2016, PKM electronic GmbH
Radiocommunications (Electromagnetic Compatibility) Standard 2008
EN 55022: 2010
Report No.: 16/06-0033 Dated: 18 August 2016, PKM electronic GmbH
Radiocommunications (Electromagnetic Radiation – Human Exposure) Standard 2014
Maximum Exposure Levels to Radio Frequency Fields – 3 kHz to 300 GHz (2002) RPS 3, ARPANSA
Exemption– Fixed Station Exemption, ARPANSA Schedule 5, General Public Exposure, <20mW Mean Power.

OEM products that this module may be installed may also be required to show compliance with Radiocommunications (Short Range Devices) Standard 2014 (Amnt 1 : 2015), Radiocommunications (Electromagnetic Compatibility) Standard 2008, the Radiocommunications (Electromagnetic Radiation – Human Exposure) Standard 2014 and the requirements of the Telecommunications Labelling Notice.


Declaration

I hereby declare that:

1. I am authorised to make this declaration on behalf of the Company mentioned above,
2. the contents of this form are true and correct, and
3. the product mentioned above complies with the applicable above mentioned standards and all products supplied under this declaration will be identical to the product identified above.

Note: Under section 137.1 of the *Criminal Code Act 1905*, it is an offence to knowingly provide false or misleading information to a Commonwealth entity.

Penalty: 12 months Imprisonment

 Signature of Supplier or Agent Robert Norris Print Name	General Manager Position In Organisation 28th November 2017 Date
---	--

The *Privacy Act 1988* (Cth) (the *Privacy Act*) imposes obligations on the ACMA in relation to the collection, security, quality, access, use and disclosure of personal information. These obligations are detailed in the Australian Privacy Principles.

The ACMA may only collect personal information if it is reasonably necessary for, or directly related to, one or more of the ACMA's functions or activities.

The purpose of collecting the personal information in this form is to ensure the supplier is identified in the 'Declaration of conformity'. If this Declaration of Conformity is not completed and the requested information is not provided, a compliance label cannot be applied.

Further information on the Privacy Act and the ACMA's Privacy Policy is available at www.acma.gov.au/privacypolicy. The Privacy Policy contains details about how you may access personal information about you that is held by the ACMA, and seek the correction of such information. It also explains how you may complain about a breach of the Privacy Act and how we will deal with such a complaint.

Should you have any questions in this regard, please contact the ACMA's privacy contact officer on telephone on 1800 226 667 or by email at privacy@acma.gov.au.

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

A Parsing ESRPB / EDRPB radio telegrams

This appendix is intended as an example of how start to parse received ESRPB / EDRPB radio telegrams. Please refer to chapter 4 first for a description of the BLE frame structure.

A.1 Data telegram example

We consider the following raw data telegram data captured from an EnOcean EDRPB device:

D6 BE 89 8E 42 13 9F 1B 00 00 15 E2 0C FF DA 03 69 01 00 00 10 8A D6 C1 7E 16 EE 23

A.1.1 BLE frame structure

The message shown above can be parsed into the following components (keep in mind the little endian byte order):

BLE Access Address (4 byte):	0x8E89BED6
BLE Frame Control (2 byte):	0x1342 Size of source address + payload: 0x13 (19 byte) Telegram type: Non-connectable Advertising
BLE Source Address (6 byte):	0xE21500001B9F
Length of payload (1 byte):	0x0C (12 byte)
Type of payload (1 byte):	0xFF (manufacturer-specific data)
Manufacturer ID (2 byte):	0x03DA (EnOcean GmbH)
EnOcean Payload (9 byte):	69 01 00 00 10 8A D6 C1 7E
CRC (3 byte):	16 EE 23

A.1.2 EnOcean data telegram payload structure

The EnOcean data telegram payload can now be parsed as follows:

Sequence Counter (4 byte):	0x00000169
Switch Status:	10 (Release of button B1)
Telegram Signature:	C7 24 EA F0

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

A.2 Commissioning telegram example

We consider the following raw commissioning telegram data captured from an EnOcean PTM 215B device:

```
D6 BE 89 8E 42 24 9F 1B 00 00 15 E2 1E FF DA 03 71 01 00 00 AB 4B 9A 91 85 2B 70 B8
A6 52 A0 5E 92 BB 12 A0 9F 1B 00 00 15 E2 9E 6D 7C
```

A.2.1 BLE frame structure

The message shown above can be parsed into the following components (keep in mind the little endian byte order):

BLE Access Address (4 byte):	0x8E89BED6
BLE Frame Control (2 byte):	0x2442 Size of source address + payload: 0x24 (36 byte) Telegram type: Non-connectable Advertising
BLE Source Address (6 byte):	0xE21500001B9F
Length of payload (1 byte):	0x1E (30 byte)
Type of payload (1 byte):	0xFF (manufacturer-specific data)
Manufacturer ID (2 byte):	0x03DA (EnOcean GmbH)
EnOcean Payload (27 byte):	71 01 00 00 AB 4B 9A 91 85 2B 70 B8 A6 52 A0 5E 92 BB 12 A0 9F 1B 00 00 15 E2
CRC (3 byte):	0x7C6D9E

A.2.2 EnOcean commissioning telegram payload structure

The EnOcean commissioning telegram payload can now be parsed as follows:

Sequence Counter (4 byte):	0x00000171
Security Key:	AB 4B 9A 91 85 2B 70 B8 A6 52 A0 5E 92 BB 12 A0
Static Source Address:	0xE21500001B9F

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

B Authentication of ESRPB / EDRPB data telegrams

ESRPB / EDRPB provide the option to authenticate its data telegrams as described in chapter 4.8. The authentication mechanism used by the PTM 215B module in ESRPB / EDRPB is standardized as RFC3610. The full RFC3610 specification could be found here at the time of writing and should be used as primary source of information: <https://www.ietf.org/rfc/rfc3610.txt>

The following description aims to summarize the security processing steps for users not deeply familiar with cryptography in general or RFC3610 in particular.

B.1 Algorithm input parameters

The purpose of the security processing in PTM 215B 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.

To do so, two types of algorithm parameters are required:

- **Constant algorithm input parameters**
These parameters identify high level algorithm and telegram properties and are the same for any PTM 215B telegram
- **Variable algorithm input parameters**
These parameters identify telegram-specific parameters and therefore depend on the specifics of the transmitted telegram

B.1.1 Constant input parameters

The RFC3610 implementation in PTM 215B requires two constant input parameters:

- **Length field size**
This is the size (in byte) of the field used to encode the length of the input data (which is the payload to be authenticated).
The maximum size of PTM 215B payload to be authenticated is 13 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**
This is the desired size of the generated signature which is 4 byte for PTM 215B

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 6 – Constant algorithm input parameters

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

B.1.2 Variable input parameters

The RFC3610 implementation in PTM 215B requires four variable input parameters:

- **Source address**
The 6 byte source address used to identify the sender of an authenticated message. The source address is required in little endian (least significant byte first) format.
- **Input data (Payload to be authenticated)**
The authenticated payload contains source address, sequence counter, switch status and optional data (if present). See chapter 4.8 for a description of the authenticated payload.
- **Input length (Size of the payload to be authenticated)**
The length of the payload to be authenticated depends on the amount of optional data used in the telegram. This is configured via the Configuration register, see chapter 6.7.6.
By default, no optional data is present and the length of the authenticated payload is 9 byte.
- **Sequence counter**
Each PTM 215B contains a sequence counter which is initialized to zero during production and increased for each telegram that is sent.
The sequence counter is transmitted as part of the input data.
The receiver of PTM 215B telegrams keeps track of this counter and will accept only telegrams with counter values higher than the highest previously used value. This eliminates the possibility of reusing previously transmitted telegrams.
Note that the individual (identical) advertising telegrams used to encode the same data telegram use the same sequence counter value.
- **Security key**
Each PTM 215B is programmed with a random 16 byte security key during manufacturing. This key can be modified using the NFC interface, see chapter 6.7.3.

Parameter	Comment / Description	Example
Source Address	Unique source address of the PTM 215B module (little endian)	B819000015E2 (little endian representation of E215000019B8)
Input Data	Telegram data to be authenticated	0CFFDA03D00A000003
Input Length	Length of input data (in bytes, encoded using 2 bytes)	0x0009 (if optional data size = 0, default) 0x000A (if optional data size = 1) 0x000B (if optional data size = 2) 0x000D (if optional data size = 4)
Sequence Counter	Incrementing counter to avoid replay Part of the input data (byte 4 ... 7)	D00A0000 (little endian representation of the counter value 0000AD0)
Security Key	128 bit random key that is known both to sender and receiver	3DDA31AD44767AE3CE56DCE2B3CE2ABB

Table 7 – Variable input parameters

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

B.1.3 Obtaining the security key

All required parameters except the security key can be directly extracted from the received message that shall be authenticated.

The security key –the common secret shared between sender and receiver – has to be obtained via specific mechanisms. As described in chapter 5, there are three different ways to obtain the security key of a given PTM 215B module:

- Obtaining the key via the NFC configuration interface
- Obtaining the key via the product DMC code
- Obtaining the key via a dedicated commissioning telegram

Each option is described now in detail.

B.1.3.1 Obtaining the security key via NFC interface

Using the Elatec TWN4 reader (as described in chapter 6.3), the security key can be read using the following command sequence:

```
SearchTag(32)
NTAG_PwdAuth(0x00 0x00 0xE2 0x15,0x00 0x00)
NTAG_Read(0x14)
```

This is equivalent to the following binary command sequence:

```
Request: 050020
Response: 0001803807048831A2014F8020060000E2150000

Request: 20060000E2150000
Response: 0001

Request: 200014
Response: 00013DDA31AD44767AE3CE56DCE2B3CE2ABB
```

The tag response to the last command - NTAG_Read(0x14) - contains the password:

```
NTAG_Read(0x14)    Result: true    Page: 3DDA31AD44767AE3CE56DCE2B3CE2ABB
```

The password of this device is therefore: 3DDA31AD44767AE3CE56DCE2B3CE2ABB

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

B.1.3.2 Obtaining the security key via the product DMC code

Each ExRPB product is marked using a DMC code on its product label as described in chapter 5.2. The security key is encoded in the "Z" field.

B.1.3.3 Obtaining the security key via a commissioning telegram

PTM 215B modules can send dedicated commissioning telegrams that identify their security key. Transmission of such commissioning telegrams can be triggered by means of a specific button sequence as described in chapter 5.3.

Note that this feature can be disabled via the NFC commissioning interface by setting the Disable Radio Commissioning flag in the Configuration register to 0b1 (see chapter 6.7.6).

The resulting commissioning telegram has the following payload:

```
1D FF DA 03 56 04 00 00 3D DA 31 AD 44 76 7A E3 CE 56 DC E2 B3 CE 2A BB B8 19 00 00  
15 E2
```

Please see Figure 20 in chapter 5.3.2 for a description of the commission telegram structure. The location of the security key is for reference highlighted red above. This means that the security key of this device is:

3DDA31AD44767AE3CE56DCE2B3CE2ABB

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

B.2 Internal parameters

The RFC3610 implementation in PTM 215B derives a set of internal parameters for further processing from the provided input parameters.

Again, there are two types of internal parameters:

- **Constant internal parameters**
 These parameters are based on the high level algorithm and telegram properties and are the same for any PTM 215B telegram
- **Variable input parameters**
 These parameters are based on the telegram-specific parameters and therefore depend on the specifics of the transmitted telegram

B.3 Constant internal parameters

The RFC3610 implementation in PTM 215B derives two internal parameters – M' and L' – based on the input data 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 8 below - is the same for all PTM 215B telegrams.

Parameter	Comment / Description	Example
M'	Binary encoded output length $M' = (\text{Output length} / 2) - 1$	0b001 (always)
L'	Binary encoded length field size $L' = \text{length field size} - 1$	0b001 (always)
$A0_Flag$	L'	0x01 (always)
$B0_Flag$	$(0b01 \ll 6) + (M' \ll 3) + L'$	0x49 (always)
i	Iteration counter	0x0000 (always)

Table 8 – Constant internal parameters

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

B.4 Variable internal parameters

The RFC3610 implementation in PTM 215B derives four internal parameters – Nonce, A0, B0 and B1 – based on the telegram specific input data and the constant internal parameters.

These variable internal parameters - listed in Table 9 below - are then used together with the security key to calculate the actual signature.

Parameter	Comment / Description	Example
Nonce	13 byte initialization vector based on concatenation of source address, sequence counter and padding, see 4.8.1	FE19000015E2D00A000000000000
A0	A0_Flag followed by Nonce followed by 2 byte 0x00	01FE19000015E2D00A00000000000000
B0	B0_Flag followed by Nonce followed by 2 byte 0x00 (no message to encode)	49FE19000015E2D00A00000000000000
B1	Input Length followed by Input Data followed by 5 / 4 / 3 / 1 byte of 0x00 padding (for optional data size = 0 / 1 / 2 / 4 byte)	00090CFFDA03D00A000000300000000000

Table 9 – Variable internal parameters

B.5 Algorithm execution sequence

The algorithm uses the variable internal parameters A_0, B_0, B_1 together with the private key to generate the authentication vector T_0 using three AES-128 and two XOR operations. The algorithm execution sequence is shown in Figure 32 below.

The first four bytes of T_0 are then used to authenticate PTM 215B telegrams.

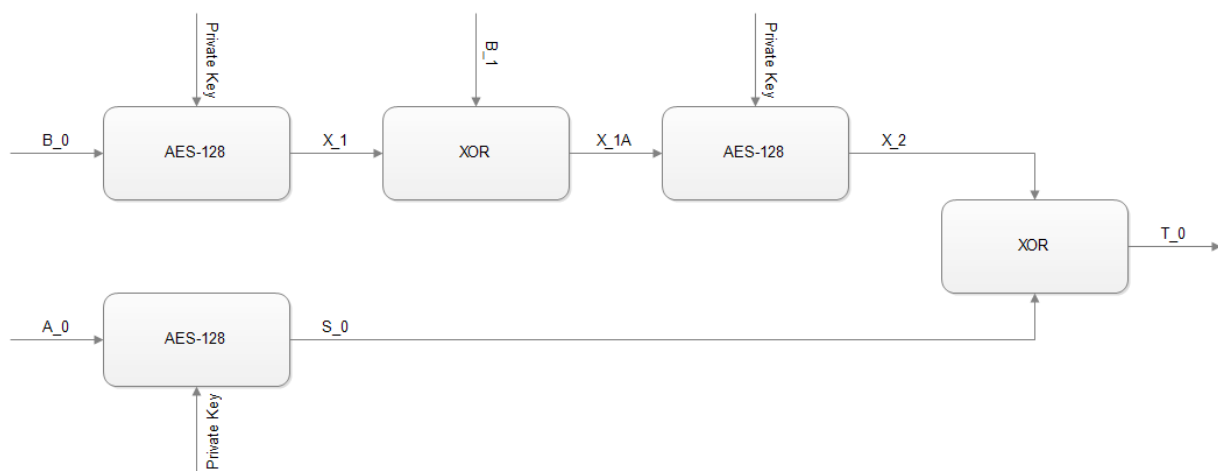


Figure 32 – Authentication algorithm sequence

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

B.6 Examples

The following four chapters give step by step examples based on one actual device and 0 / 1 / 2 or 4 byte of optional data.

At the time of writing, a suitable online AES calculator could be found here:

<http://testprotect.com/appendix/AEScalc>

Likewise, a suitable XOR calculator could be found here:

<http://xor.pw/>

B.6.1 Data telegram without optional data

For this example, we consider the following telegram payload received from a PTM 215B with the source address E215000019B8 and security key 3DDA31AD44767AE3CE56DCE2B3CE2ABB:

0C FF DA 03 5D 04 00 00 11 B2 FA 88 FF

The last four bytes of this payload (B2 FA 88 FF) are the sender-provided signature which has to be authenticated (compared against the signature the receiver calculates based on its own security key).

The variable input parameters are therefore the following:

Parameter	In this example
Source Address	B819000015E2 (little endian representation of E215000019B8)
Input Data	0CFFDA035D04000011
Input Length	0x0009
Sequence Counter	5D040000
Security Key	3DDA31AD44767AE3CE56DCE2B3CE2ABB

The constant internal parameters are always the same:

Parameter	In this example
A0_Flag	0x01 (always)
B0_Flag	0x49 (always)
i	0x0000 (always)

Based on variable input data and constant internal algorithm parameters, we can now derive the following variable internal parameters:

Parameter	In this example
Nonce	B819000015E25D04000000000000
A0	01B819000015E25D0400000000000000
B0	49B819000015E25D0400000000000000
B1	00090CFFDA035D040000110000000000

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

We can now calculate the signature according to the steps shown in Figure 32.

```
X_1 = AES128(B0, Key)
X_1 = AES128(49B819000015E25D0400000000000000, 3DDA31AD44767AE3CE56DCE2B3CE2ABB)
X_1 = 41ef09792ae152ae52c671435c1f247d
```

```
X_1A = XOR(X_1, B_1)
X_1A = XOR(41ef09792ae152ae52c671435c1f247d, 00090CFFDA035D040000110000000000)
X_1A = 41e60586f0e20faa52c660435c1f247d
```

```
X_2 = AES128(X1A, Key)
X_2 = AES128(41e60586f0e20faa52c660435c1f247d, 3DDA31AD44767AE3CE56DCE2B3CE2ABB)
X_2 = 8d89e733da516ae3e08f9e30184909fc
```

```
S_0 = AES128(A0, Key)
S_0 = AES128(01B819000015E25D0400000000000000, 3DDA31AD44767AE3CE56DCE2B3CE2ABB)
S_0 = 3f736fcc8bcaf2d4aabca0260fab7976
```

```
T_0 = XOR(X_2, S_0)
T_0 = XOR(8d89e733da516ae3e08f9e30184909fc, 3f736fcc8bcaf2d4aabca0260fab7976)
T_0 = b2fa88ff519b98374a333e1617e2708a
```

The calculated signature is formed by the first four bytes of T_0, i.e. it is B2 FA 88 FF.

The calculated signature matches the signature that was transmitted as part of the payload. This proves that the telegram originates from a sender that possesses the same security key and the telegram content has not been modified.

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

B.6.2 Data telegram with 1 byte optional data

For this example, we consider the following telegram payload received from a PTM 215B with the source address E215000019B8 and security key 3DDA31AD44767AE3CE56DCE2B3CE2ABB:

0D FF DA 03 62 04 00 00 10 12 B9 FE AC C1

The last four bytes of this payload (B9 FE AC C1) are the sender-provided signature which has to be authenticated. The variable input parameters are therefore the following:

Parameter	In this example
Source Address	B819000015E2 (little endian representation of E215000019B8)
Input Data	0DFFDA03620400001012
Input Length	0x000A
Sequence Counter	62040000
Security Key	3DDA31AD44767AE3CE56DCE2B3CE2ABB

Based on variable input data and constant internal algorithm parameters, we can now derive the following variable internal parameters:4

Parameter	In this example
Nonce	B819000015E26204000000000000
A0	01B819000015E2620400000000000000
B0	49B819000015E2620400000000000000
B1	000A0DFFDA0362040000101200000000

We can now calculate the signature as follows:

```
X_1 = AES128(B0, Key)
X_1 = AES128(49B819000015E2620400000000000000, 3DDA31AD44767AE3CE56DCE2B3CE2ABB)
X_1 = dc8d685f968e795b23f4370b3091f33f
```

```
X_1A = XOR(X_1, B_1)
X_1A = XOR(dc8d685f968e795b23f4370b3091f33f, 000A0DFFDA0362040000101200000000)
X_1A = dc8765a04c8d1b5f23f427193091f33f
```

```
X_2 = AES128(X1A, Key)
X_2 = AES128(dc8765a04c8d1b5f23f427193091f33f, 3DDA31AD44767AE3CE56DCE2B3CE2ABB)
X_2 = 231be2ff54ca62fb38d32eaaaf1b447d
```

```
S_0 = AES128(A0, Key)
S_0 = AES128(01B819000015E2620400000000000000, 3DDA31AD44767AE3CE56DCE2B3CE2ABB)
S_0 = 9ae54e3e95de9f91a0c279537bc25b00
```

```
T_0 = XOR(X_2, S_0)
T_0 = XOR(231be2ff54ca62fb38d32eaaaf1b447d, 9ae54e3e95de9f91a0c279537bc25b00)
T_0 = b9feacc1c114fd6a981157f9d4d91f7d
```

The calculated signature is formed by the first four bytes of T_0, i.e. it is B9 FE AC C1.

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

B.6.3 Data telegram with 2 byte optional data

For this example, we consider the following telegram payload received from a PTM 215B with the source address E215000019B8 and security key 3DDA31AD44767AE3CE56DCE2B3CE2ABB:

0E FF DA 03 63 04 00 00 11 12 34 52 E0 51 16

The last four bytes of this payload (52 E0 51 16) are the sender-provided signature which has to be authenticated. The variable input parameters are therefore the following:

Parameter	In this example
Source Address	B819000015E2 (little endian representation of E215000019B8)
Input Data	0EFFDA0363040000111234
Input Length	0x000B
Sequence Counter	62040000
Security Key	3DDA31AD44767AE3CE56DCE2B3CE2ABB

Based on variable input data and constant internal algorithm parameters, we can now derive the following variable internal parameters:

Parameter	In this example
Nonce	B819000015E26304000000000000
A0	01B819000015E2630400000000000000
B0	49B819000015E2630400000000000000
B1	000B0EFFDA0363040000111234000000

We can now calculate the signature as follows:

$X_1 = \text{AES128}(B0, \text{Key})$
 $X_1 = \text{AES128}(49B819000015E2630400000000000000, 3DDA31AD44767AE3CE56DCE2B3CE2ABB)$
 $X_1 = \text{ab5ec24beabc9ddeeb73751c7734cc64}$

$X_1A = \text{XOR}(X_1, B_1)$
 $X_1A = \text{XOR}(\text{ab5ec24beabc9ddeeb73751c7734cc64}, 000B0EFFDA0363040000111234000000)$
 $X_1A = \text{ab55ccb430bffedaeb73640e4334cc64}$

$X_2 = \text{AES128}(X1A, \text{Key})$
 $X_2 = \text{AES128}(\text{ab55ccb430bffedaeb73640e4334cc64}, 3DDA31AD44767AE3CE56DCE2B3CE2ABB)$
 $X_2 = \text{d33e96d7a105c4e8543207f9e75e6cfe}$

$S_0 = \text{AES128}(A0, \text{Key})$
 $S_0 = \text{AES128}(01B819000015E2630400000000000000, 3DDA31AD44767AE3CE56DCE2B3CE2ABB)$
 $S_0 = \text{81dec7c16915c6647d92b0668f65e9c9}$

$T_0 = \text{XOR}(X_2, S_0)$
 $T_0 = \text{XOR}(\text{d33e96d7a105c4e8543207f9e75e6cfe}, \text{81dec7c16915c6647d92b0668f65e9c9})$
 $T_0 = \text{52e05116c810028c29a0b79f683b8537}$

The calculated signature is formed by the first four bytes of T_0 , i.e. it is 52 E5 11 16.

ESRPB / EDRPB - EASYFIT BLUETOOTH® SINGLE / DOUBLE ROCKER PAD

B.6.4 Data telegram with 4 byte optional data

For this example, we consider the following telegram payload received from a PTM 215B with the source address E215000019B8 and security key 3DDA31AD44767AE3CE56DCE2B3CE2ABB:

10 FF DA 03 6A 04 00 00 10 12 34 56 78 2C 9E 10 95

The last four bytes of this payload (2C 9E 10 95) are the sender-provided signature which has to be authenticated. The variable input parameters are therefore the following:

Parameter	In this example
Source Address	B819000015E2 (little endian representation of E215000019B8)
Input Data	10FFDA036A0400001012345678
Input Length	0x000D
Sequence Counter	6A040000
Security Key	3DDA31AD44767AE3CE56DCE2B3CE2ABB

Based on variable input data and constant internal algorithm parameters, we can now derive the following variable internal parameters:

Parameter	In this example
Nonce	B819000015E26A04000000000000
A0	01B819000015E26A0400000000000000
B0	49B819000015E26A0400000000000000
B1	000D10FFDA036A040000101234567800

We can now calculate the signature as follows:

```
X_1 = AES128(B0, Key)
X_1 = AES128(49B819000015E26A0400000000000000, 3DDA31AD44767AE3CE56DCE2B3CE2ABB)
X_1 = 434fa5855b8a8a8ae99bf1cb114a51b7
```

```
X_1A = XOR(X_1, B_1)
X_1A = XOR(434fa5855b8a8a8ae99bf1cb114a51b7, 000D10FFDA036A040000101234567800)
X_1A = 4342b57a8189e08ee99be1d9251c29b7
```

```
X_2 = AES128(X1A, Key)
X_2 = AES128(4344b57a8189e08ee99be1d9251c29b7, 3DDA31AD44767AE3CE56DCE2B3CE2ABB)
X_2 = 12c78b85a4ecb6f34daff7651db8e386
```

```
S_0 = AES128(A0, Key)
S_0 = AES128(01B819000015E2630400000000000000, 3DDA31AD44767AE3CE56DCE2B3CE2ABB)
S_0 = 3e599b103f33447e6b46eec4a042d0bc
```

```
T_0 = XOR(X_2, S_0)
T_0 = XOR(12c78b85a4ecb6f34daff7651db8e386, 3e599b103f33447e6b46eec4a042d0bc)
T_0 = 2c9e10959bdf28d26e919a1bdfa333a
```

The calculated signature is formed by the first four bytes of T_0, i.e. it is 2C 9E 10 95.