VIMAR

Installer Manual

03925

4-button flat device with 2.4 GHz *Bluetooth® technology* Low Energy standard radiofrequency transmitter, energy harvesting supply powered by built-in electrodynamic generator, to complete with Eikon 20506 or 20506.2, Arké 19506 or 19506.2 or Plana 14506 or 14506.2 buttons - 2 modules.

HOME AUTOMATION

Index

1. General description

1.1 Basic functionality

03925 enables the realization of energy harvesting wireless switches for building or industrial automation systems communicating based on ***Bluetooth technology*** low energy technology.

03925 pushbutton transmitters are self-powered (no batteries) and fully maintenancefree. They can therefore be used in all environments including locations that are difficult to reach or within hermetically sealed housings. The required energy is generated by an electro-dynamic energy transducer actuated by an energy bow located on the left and right of the module. This energy bow which can be pushed from outside the module by an appropriate pushbutton or switch rocker.

When the energy bow is pushed down or released, electrical energy is created and a radio telegram according to the ***Bluetooth technology*** low energy standard is transmitted. This radio telegram transmits the status of all four contact nipples at the moment when the energy bow was pushed down or released.

03925 radio telegrams are protected with AES-128 security based on a device-unique private key.

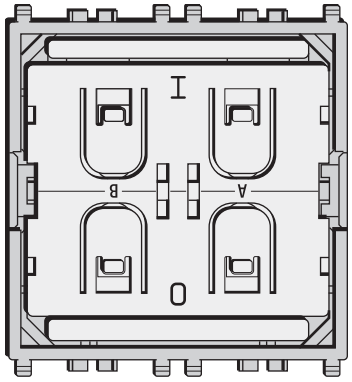

Fig. 1: 03925

1.2 Technical data

Antenna	Integrated PCB antenna
Max. transmit power measured	0.4dBm / 1.1mW
Communication Range (Guidance Only)	75 m ideal line of sight / 10 m indoor environment
Communication Standard	*Bluetooth technology* Low Energy (BLE)
Radio Frequency (min / max)	2402 MHz / 2480 MHz
Default Radio Channels	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
Button Inputs	Up to four buttons or two rockers

1.3 Environmental conditions

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

2. Functional information

2.1 03925 Device Overview

The pushbutton transmitter module 03925 enables the implementation of wireless remote controls without batteries. It transmits ***Bluetooth technology*** Low Energy (BLE) data telegrams where the required energy is provided by a built-in electro-dynamic energy generator.

The outer appearance of 03925 is shown in Figure 2 below.

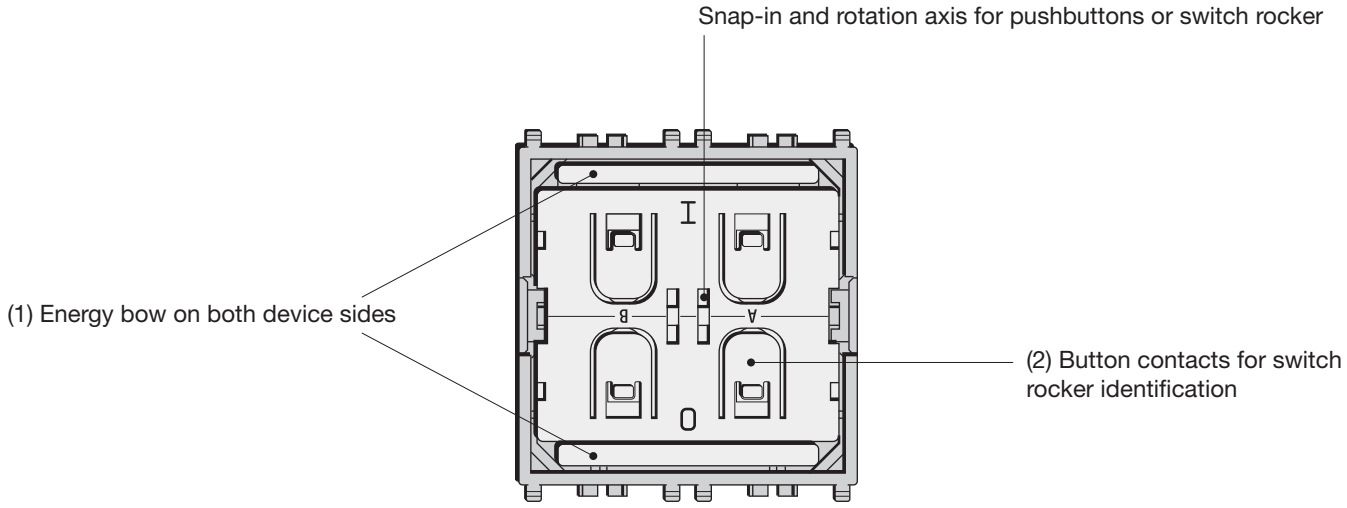

Fig. 2: Electro-dynamic powered pushbutton transmitter module 03925

2.2 Basic Functionality

03925 devices contain an electro-dynamic energy converter which is actuated by an energy bow (1). This bow is pushed by an appropriate push button, switch rocker or a similar construction mounted onto the device. An internal spring will release the energy bow as soon as it is not pushed down anymore.

When the energy bow is pushed down, electrical energy is created and a BLE radio telegram is transmitted which identifies the action (pressed or not pressed) and the status of the four button contacts (2). Releasing the energy bow similarly generates energy which is used to transmit a different radio telegram.

It is therefore possible to distinguish between radio telegrams sent when the energy bar was pushed and radio telegrams sent when the energy bar was released.

By identifying these different telegrams types and measuring the time between pushing and releasing of the energy bar, it is possible to distinguish between “Long” and “Short” button contact presses. This enables simple implementation of applications such as dimming control or blinds control including slat action.

2.3 User Interface

03925 devices provide four button contacts. They are grouped into two channels (Channel A and Channel B) each containing two button contacts (State O and State I).

The state of all four button contacts (pressed or not pressed) is transmitted together with a unique device identification (48 Bit device ID) whenever the energy bow is pushed or released.

Figure 3 below shows the arrangement of the four button contacts and their designation:

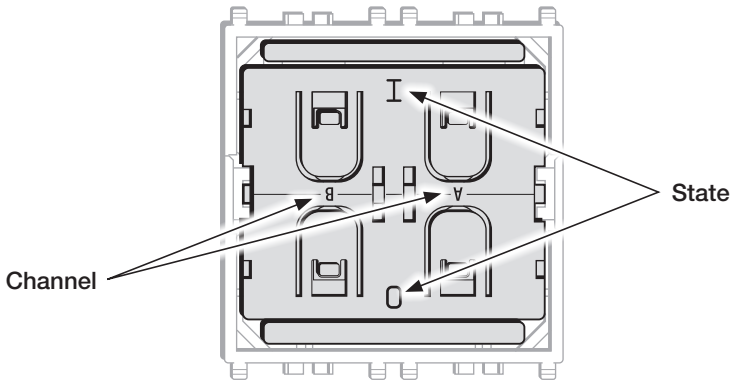

Fig. 3: Button contact designation

3. Telegram transmission

3.1 Radio channel parameters

03925 transmits ***Bluetooth technology*** Low Energy (BLE) advertising telegrams within the 2.4 GHz radio frequency band (2402MHz … 2480MHz).

By default, 03925 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 6.7.9.

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 03925.

Radio Channel	Frequency	Channel Type
BLE Radio Channel		
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 – 03925 supported radio channels

3.2 Default radio transmission sequence

03925 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, 03925 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.

03925 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.

Telegram transmission

The selection of the transmission mode is done using the CUSTOM_VARIANT register of the NFC configuration interface as described in chapter 6.7.8.

03925 supports the following user-defined sequences:

- Three channels 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 channels sequence is described in chapter 3.3.1 below.
- Two channels 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 channels sequence

The three channels 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 registers CH_REG1, CH_REG2 and CH_REG3.

The 03925 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 channels radio transmission sequence

The format of CH_REG1, CH_REG2 and CH_REG3 is described in chapter 6.7.9.

3.3.2 Two channels sequence

The two channels 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 03925 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 channels radio transmission sequence

The format of CH_REG1 and CH_REG2 is described in chapter 6.7.9.

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 03925 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 6.7.9.

4. Telegram format

03925 transmits ***Bluetooth technology*** Low Energy (BLE) radio telegrams in the 2.4 GHz band. For detailed information about the ***Bluetooth technology*** Low Energy 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 – Default radio transmission sequence

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.

Bit 15 (MSb)					Bit 0 (LSb)
UNUSED (2 Bit)	LENGTH (6 Bit)	RX ADDR (1 Bit)	TX ADDR (1 Bit)	UNUSED (2 Bit)	TYPE (4 Bit)
00	Length of Address + Payload	0: Not used	1: Random	00	0010: TX-only Advertising (ADV_NONCONN_IND)

Figure 9 – BLE header structure

4.4 Source address

The 6 byte BLE Source Address (MAC address) uniquely identifies each 03925 product.

03925 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

03925 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 6.7.7) to 0b0.

These two address modes are described in the following chapters.

4.4.1 Static source address mode

By default, 03925 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 03925 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 03925 devices. 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 6.7.3

Figure 10 below illustrates the static address structure used by 03925.

Product Type ID (16 Bit)	Unique Device Address (32 Bit)
0xE215	
MSB	LSB

Figure 10 – BLE static source address structure

4.4.2 Private resolvable source address mode

For some applications it is desirable to modify (rotate) the source address used by 03925 in order to prevent tracking of its radio transmissions. At the same time, each 03925 device must remain uniquely identifiable by the receiver.

To achieve these goals, 03925 can be configured via NFC to use random resolvable private addresses.

Using random resolvable private addresses requires that both 03925 and the receiver both know a common key – the so-called Identity Resolution Key (IRK). 03925 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.

prand (24 Bit)			hash (24 Bit)
0	1	Random Data (22 Bit)	
MSB			LSB

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.

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.

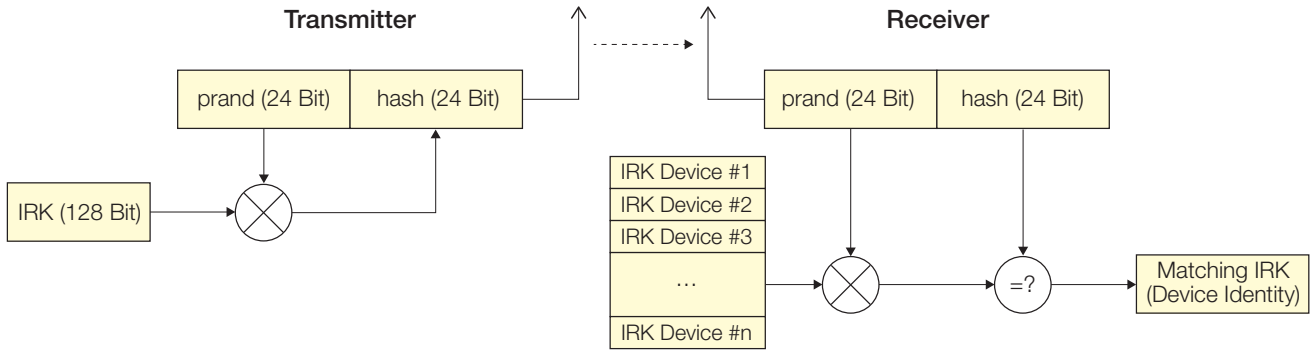

Figure 12 – Resolving private source addresses

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.

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 03925 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. Vimar has been assigned 0x03DA as manufacturer ID code. The Manufacturer ID can be changed via the NFC configuration interface as described in chapter 6.7.5.
- 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)
  03925 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 6.7.7.
- Security Signature (4 byte)
  The Security Signature is used to authenticate 03925 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

4.7 Switch status encoding

The Switch Status field within the Payload data identifies the 03925 action (button push or release). 03925 uses the following sequence to identify and transmit button contact status:

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

In 03925, 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 03925 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
Shal 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 – 03925 button action encoding

4.8 03925 telegram authentication

03925 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.

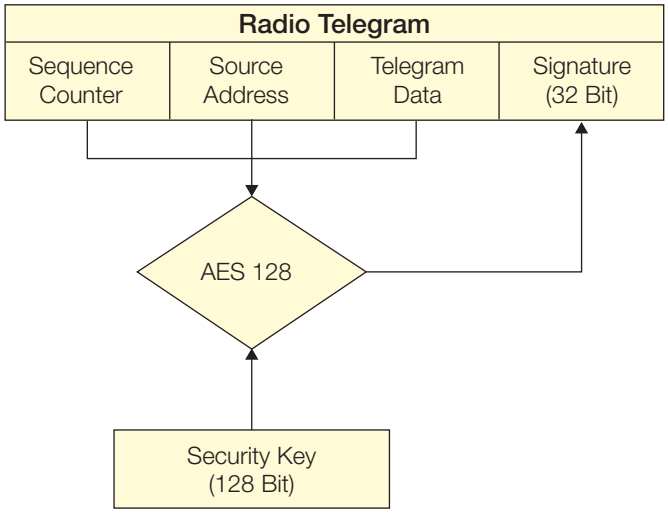

Figure 15 – Telegram authentication flow

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 03925 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 (03925) 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 03925 and only accepts messages with higher sequence counter values (i.e. not accepts equal or lower sequence counter values for subsequent telegrams).

4.8.1 Authentication implementation

03925 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.

5. Commissioning

Commissioning is the process by which 03925 is learned into a receiver (actuator, controller, gateway, etc.).

The following two tasks are required in this process:

- Device identification
  The receiver needs to know how to uniquely identify this specific 03925 device. This is achieved by using a unique 48 Bit ID (Source Address) for each 03925 device as described in chapter 4.4. In addition, up to 4 byte of Optional Data can be configured as described in chapter 6.7.6.
- Security parameter exchange
  The receiver needs to be able to authenticate radio telegrams from 03925 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 03925 to authenticate its radio telegrams.

03925 provides the following options for these tasks:

- NFC-based commissioning
  The 03925 parameters are read by a suitable commissioning tool (e.g. NFC smartphone with suitable software) which is already part of the network into which 03925 will be commissioned. The commissioning tool then communicates these parameters to the intended receiver of 03925 radio telegrams. NFC-based commissioning is described in chapter 6.
- Camera-based commissioning
  Each 03925 module contains an optically readable Data Matrix Code (DMC) which identifies its ID and its security key. This DMC can be read by a by a suitable commissioning tool (e.g. smartphone) which is already part of the network into which 03925 will be commissioned. The commissioning tool then communicates these parameters to the intended receiver of 03925 radio telegrams.
- Radio-based commissioning
  03925 can communicate its parameters via special radio telegrams (commissioning telegrams) to the intended receiver. To do so, 03925 can be temporarily placed into radio-based commissioning mode as described in chapter 5.3.

5.1 NFC-based commissioning

All required 03925 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 in 03925 uses a Mifare Ultralight tag.

Commissioning via NFC should follow these steps:

1. Unlock 03925 using the default NFC PIN code 0x0000E215
2. Read the 03925 Source Address, Security Key and Sequence Counter and configure the receiver accordingly
3. Important: The pre-programmed random security key used by 03925 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 6.7.4. 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 6.7.7.
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 03925 configuration using the default PIN code. Should you lose the new NFC PIN code then 03925 can be reset to factory mode (with the default NFC PIN code) by means of a factory reset as described in chapter 0. For security reasons, this factory reset will always reset the security key to its pre-programmed value.

5.2 Camera-based commissioning

Each 03925 module contains an optically readable Commissioning Code implemented either as Data Matrix Code or as QR Code depending on the device revision.

This Commissioning Code on the device label can be scanned by a suitable commissioning tool (e.g. smartphone or PC with DMC / QR code reader) to read the static source address and the security key of the device.

The commissioning tool can the use this information to configure the intended receiver of 03925 radio telegrams.

5.3 Radio-based commissioning

For cases where both NFC and camera-based commissioning are not feasible it is possible to set 03925 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 6.7.7).

5.3.1 Commissioning mode entry

Commissioning mode is entered using a special button contact sequence. This is illustrated in Figure 18 below.

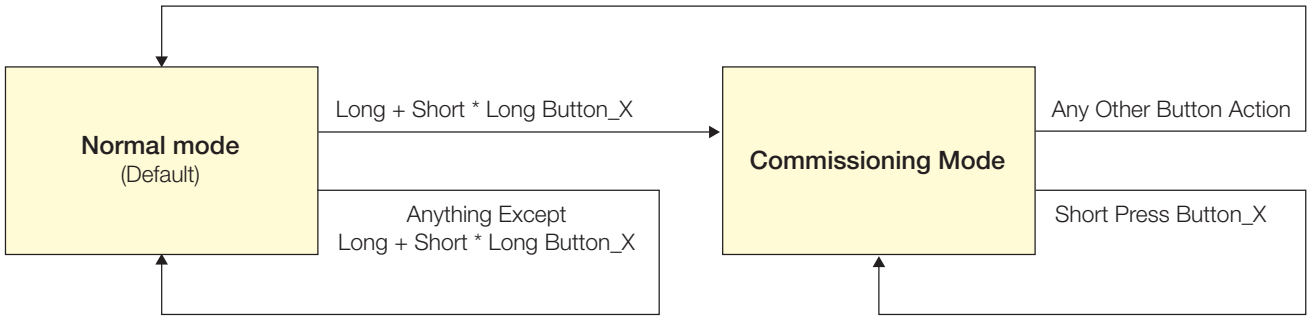

Figure 18 – Button sequence to enter radio-based commissioning mode

To enter commissioning mode, start by selecting one button contact of 03925. Any button of 03925 (A0, A1, B0, B1) can be used. This button is referred to as Button_X in Figure 18 above.

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

1. Press and hold the selected button together with the energy bar for more than 7 seconds before releasing it
2. Press the selected button together with the energy bar quickly (hold for less than 2 seconds)
3. Press and hold the selected button together with the energy bar again for more than 7 seconds before releasing it Upon detection of this sequence, 03925 will enter commissioning mode if the Disable Radio Commissioning flag in the Configuration register of the NFC interface is set to 0b0 (default state).

5.3.2 Commissioning telegram transmission

03925 will transmit a commissioning telegram (on the radio channels selected as described in chapter 3.1) upon entering commissioning mode.

03925 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 03925 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 (GmbH). This field can be changed via the NFC configuration interface as described in chapter 6.7.5.
- 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 03925 device 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 03925 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 03925. The Static Source Address is therefore again transmitted as part of the payload.

Figure 19 below illustrates the commissioning telegram payload.

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

Figure 19 – Commissioning telegram payload structure

5.3.3 Exit from commissioning mode

Pressing any key except the button used for entry into commissioning mode (Button_X) will cause 03925 to stop transmitting commissioning telegrams and return to normal data telegram transmission.

5.4 Factory Reset

03925 can be reset to its default settings by means of a factory reset.

This ensures that 03925 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 the 03925 module. Then, all four button contacts (A0, A1, B0 and B1) have to be pressed at the same time while the energy bow 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, 03925 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 (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.

In addition, 03925 will reset the following registers:

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

6. NFC interface

03925 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 03925 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

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 20 below shows the overall state machine of the NFC interface.

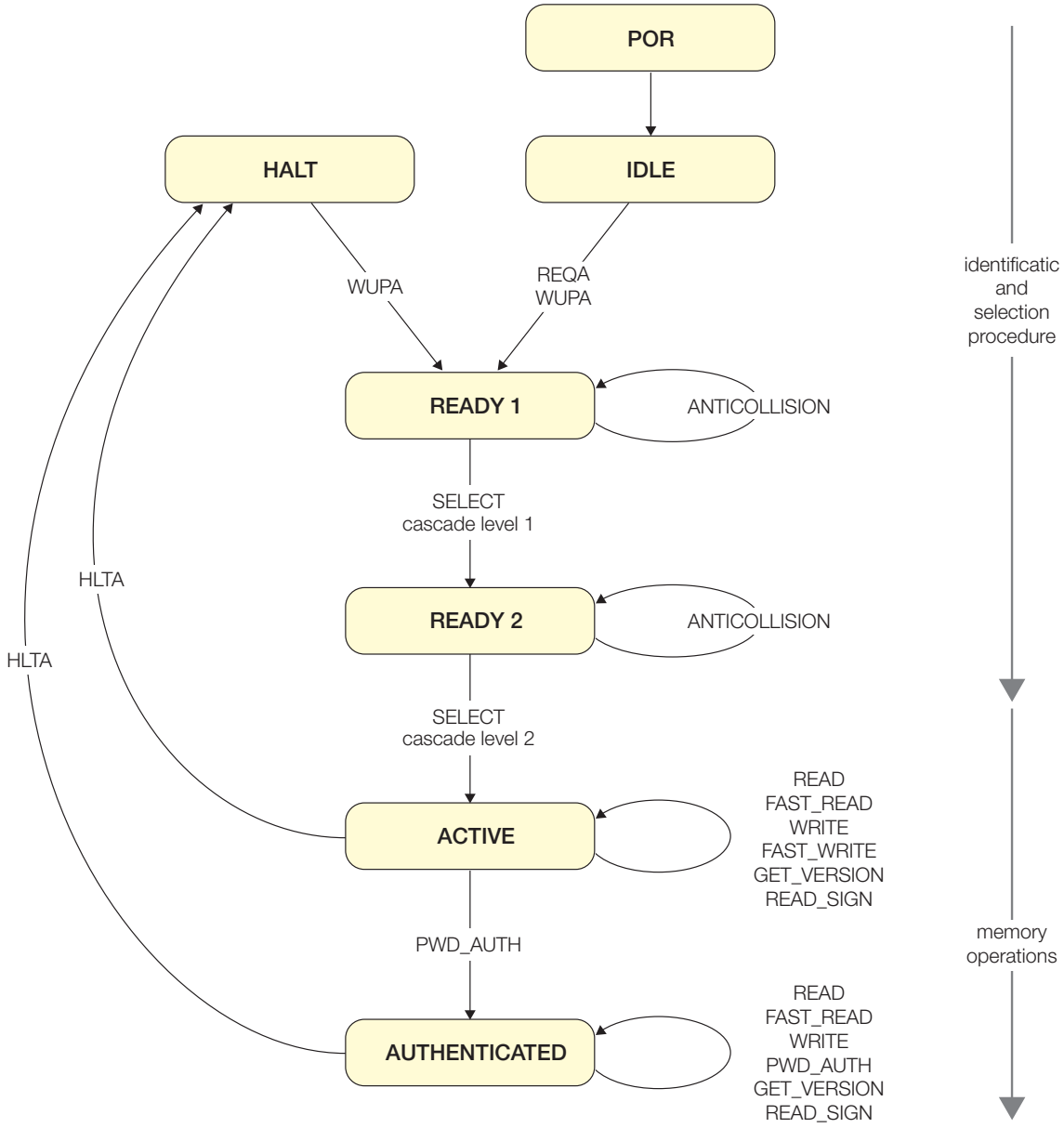

Figure 20 – NFC interface state machine

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.

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 21 below shows the read command sequence.

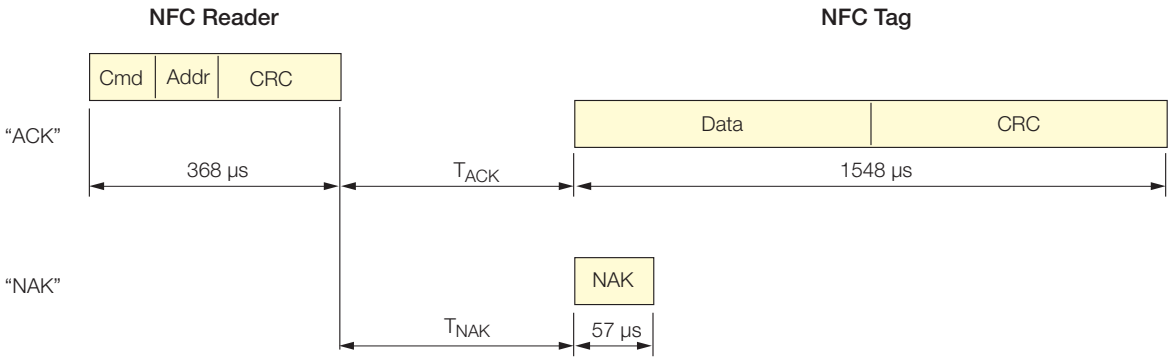

Figure 21 – NFC read command sequence

6.2.7 Write command

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

Figure 22 below shows the read command sequence.

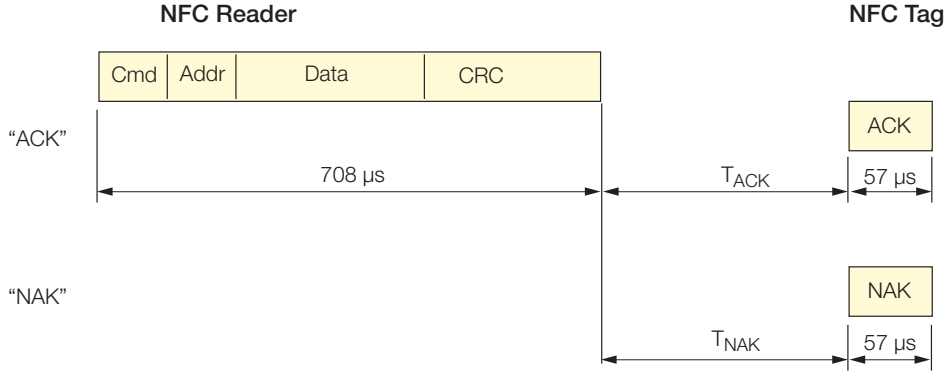

Figure 22 – NFC write command sequence

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 23 below shows the password authentication sequence.

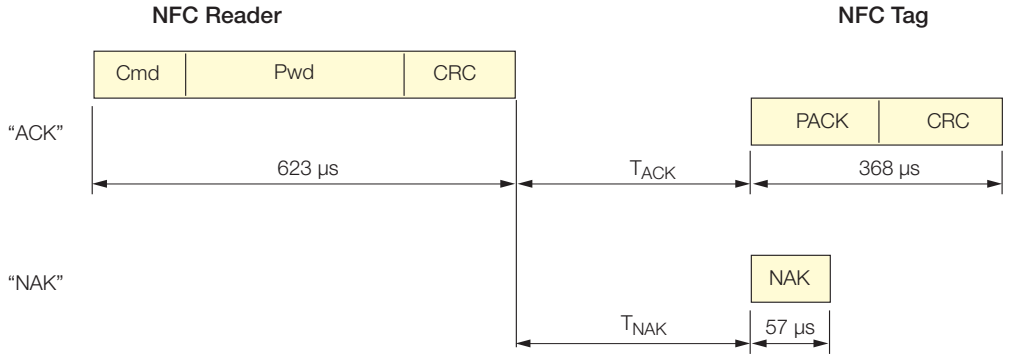

Figure 23 – Password authentication sequence

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.

6.3 Configuration memory organization

The 03925 configuration memory is divided into the following areas:

- Public data
- Protected data

In addition to that, 03925 maintains a private configuration memory region used to store default parameters and confidential information which is not accessible to the user.

Figure 24 below illustrates the configuration memory organization used by 03925.

	NFC access without PIN	NFC access with PIN
Public Data	Read-only	Read-only
Product Name ("PTM 215B")		
Product ID		
Manufacturer ID		
Source Address		
Sequence Counter		
Revision (HW / SW / NFC)		
Product Data	No access	Read / Write
Source Address Write		
Manufacturer ID Write		
Product ID Write		
Security Key Write		
Optional Data		
Configuration		
Custom Variant		
Custom Radio Channel		
Custom NFC Data		
Private Data	No access	No access
Security Key		
Default Setting		

Figure 24 – Configuration memory organization

6.4 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 2 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	Variant	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	Manufacture 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 2 – Configuration memory address map

6.5 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:

- 03925 Product Name
  This is always “PTM 215B”
- 03925 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 identify his 03925 based product, see chapter 6.6.5
- 03925 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 (GmbH).
  Product ID and Manufacturer ID can be configured by the customer as required to identify his 03925 based product, see chapter 6.6.5
- 03925 Static Source Address
  This is a 4 byte field used to identify the static source address used by 03925, see chapter 4.4.1. Each 03925 is pre-programmed with an individual staticsource address.
  The Static Source Address can be configured by the customer as required to identify his 03925 based product, see chapter 6.6.3
- 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.

6.6 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 6.6.3
- Product ID Write register
  This 8 byte register is used to update the Product ID, see chapter 6.6.5
- Manufacturer ID Write register
  This 4 byte register is used to update the Manufacturer ID, see chapter 6.6.5
- Security Key Write register
  This 16 byte register is used to update the security key used by 03925, see chapter 6.6.4
- 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 03925, see chapter 6.6.7
- Custom Variant register
  This 1 byte register is used to configure the transmission behavior of 03925, see chapter 6.6.8
- Custom Radio Channel registers (CH_REG1, CH_REG2 and CH_REG3)
  These 1 byte registers are used to configure the radio channels in custom transmission mode of 03925, see chapter 6.6.9
- Custom NFC Data
  03925 reserves 64 byte for customer-specific NFC data, see chapter 6.6.10

6.6.1 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.

6.6.2 Configuration of product parameters

03925 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 the energy bar of the 03925 module.

6.6.3 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 03925 Static Source Address. The upper 16 bit of the 03925 Static Source Address are always fixed to 0xE215 to identify the device type.

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) the energy bar of 03925

03925 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, 03925 will clear the Update Source Address flag to 0b0.

6.6.4 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
   - 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

   If 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) the energy bar of 03925

03925 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, 03925 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 0x00000000000000000000 00000000000 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.

6.6.5 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 (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 03925 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 03925 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) the energy bar of 03925.

03925 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, 03925 will clear the Update Product and Manufacturer ID flag to 0b0.

6.6.6 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 03925 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.

6.6.7 Configuration register

The Configuration register is 1 byte wide and contains configuration flags.

Figure 25 below shows the structure of the Configuration register.

Optional Data Field Size 0b00 = Disabled 0b01 = 1 byte 0b10 = 2 byte 0b11 = 4 byte		Disable Radio commissioning	Prvate Source Address	Private Security Key	Update Security Key	Update Product ID + Manufacturer ID	Update Source Address
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0

Figure 25 – Configuration register structure

6.6.8 Custom Variant register

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

Table 3 below shows the supported custom radio transmission settings.

Setting	Meaning
0x00	Commissioning and data telegrams in standard Advertising Mode (Default configuration). Note: This is equivalent to 0x04 with the radio channels set to BLE CH37, CH38 and CH39.
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 3 – Custom Variant register settings

6.6.9 Radio channel selection registers

If the Custom Variant 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 4 below.

Note that two channels 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 Channel		
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 4 – Radio Channel Selection register settings

6.6.10 Customer Data

03925 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.

03925 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.

6.7 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.

6.7.1 Security Key

The Security Key field contains the 128 bit private key used for authenticating 03925 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 6.6.4.

6.7.2 Default Settings

The Default Settings field contains a backup of the following 03925 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.

7. Application information

7.1 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.

Note that interference from other radio equipment operating in the 2.4 GHz band (WiFi routers, smartphones, wireless audio and video systems, etc.) can have major impact on radio performance.

7.2 Receiver configuration

03925 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).

03925 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.

8. Installation rules

Installation should be carried out by qualified personnel in compliance with the current regulations regarding the installation of electrical equipment in the country where the products are installed.

9. Standard compliance

RED Directive.
Standards EN 60950-1, EN 301 489-17, EN 300 328, EN 62479.

Vimar SpA declares that the radio equipment complies with Directive 2014/53/EU. The full text of the EU declaration of conformity is on the product sheet available at the following Internet address: www.vimar.com.

WEEE - Information for users

If the crossed-out bin symbol appears on the equipment or packaging, this means the product must not be included with other general waste at the end of its working life. The user must take the worn product to a sorted waste center, or return it to the retailer when purchasing a new one. Products for disposal can be consigned free of charge (without any new purchase obligation) to retailers with a sales area of at least 400 m^2, if they measure less than 25 cm. An efficient sorted waste collection for the environmentally friendly disposal of the used device, or its subsequent recycling, helps avoid the potential negative effects on the environment and people's health, and encourages the re-use and/or recycling of the construction materials.

CE

03925IEN 01 1806

VIMAR
Viale Vicenza 14
36063 Marostica VI - Italy
www.vimar.com