03925 - podręcznik instalatora

Płaskie urządzenie z czterema przyciskami i nadajnikiem radiowym 2,4 GHz w standardzie Bluetooth® Low Energy. Zasilanie z odzysku energii dzięki wbudowanemu generatorowi elektrodynamicznemu. Do uzupełnienia klawiszami Eikon 20506 lub 20506.2, Arké 19506 lub 19506.2 albo Plana 14506 lub 14506.2. Szerokość: 2 moduły. Automatyka domowa.

Pełny polski przekład treści angielskiej instrukcji 03925IEN 01 1806. Tłumaczenie TRAJKOT; nie jest oficjalną polską instrukcją Vimar. Oryginalny 26-stronicowy dokument producenta, z niezmienionymi rysunkami i tabelami, dołączono na końcu. Odwołania do rysunków i stron dotyczą numeracji oryginału.

Źródło: https://www.vimar.com/irj/go/km/docs/z_catalogo/DOCUMENT/03925IEN.80268.pdf

Uwaga do przekładu: w oryginale część odwołań do rejestrów wskazuje rozdział 6.7 zamiast 6.6, występują też niespójności wskazane przy odpowiednich tabelach. Nie zastępujemy ich własnymi parametrami. Oznaczenia rejestrów, poleceń i wartości szesnastkowe zachowano.

Spis treści

1. Opis ogólny: 1.1 Podstawowe działanie; 1.2 Dane techniczne; 1.3 Warunki środowiskowe.

2. Informacje funkcjonalne: 2.1 Przegląd urządzenia 03925; 2.2 Podstawowe działanie; 2.3 Interfejs użytkownika.

3. Transmisja telegramów: 3.1 Parametry kanałów radiowych; 3.2 Domyślna sekwencja transmisji; 3.3 Sekwencje definiowane przez użytkownika.

4. Format telegramu: 4.1 Preambuła; 4.2 Adres dostępu; 4.3 Nagłówek; 4.4 Adres źródłowy; 4.5 Suma kontrolna; 4.6 Dane użytkowe; 4.7 Kodowanie stanu przycisków; 4.8 Uwierzytelnianie telegramów.

5. Uruchomienie: 5.1 Przez NFC; 5.2 Z użyciem aparatu; 5.3 Drogą radiową; 5.4 Przywracanie ustawień fabrycznych.

6. Interfejs NFC: 6.1 Korzystanie z interfejsu; 6.2 Funkcje; 6.3 Organizacja pamięci; 6.4 Mapa adresów; 6.5 Dane publiczne; 6.6 Dane chronione; 6.7 Dane prywatne.

7. Informacje dotyczące zastosowania: 7.1 Zasięg transmisji; 7.2 Konfiguracja odbiornika. 8. Zasady instalacji. 9. Zgodność z normami i WEEE.

1. Opis ogólny

1.1 Podstawowe działanie

03925 umożliwia wykonywanie bezprzewodowych przycisków z odzyskiem energii do systemów automatyki budynkowej lub przemysłowej komunikujących się z wykorzystaniem technologii Bluetooth Low Energy.

Nadajniki przyciskowe 03925 mają własne zasilanie, nie wymagają baterii i są całkowicie bezobsługowe. Mogą więc być używane w różnych środowiskach, również w miejscach trudno dostępnych lub w hermetycznie zamkniętych obudowach. Potrzebną energię wytwarza elektrodynamiczny przetwornik uruchamiany listwą generatora, znajdującą się po lewej i prawej stronie modułu. Listwę można naciskać z zewnątrz modułu odpowiednim przyciskiem lub klawiszem kołyskowym.

Naciśnięcie albo zwolnienie listwy wytwarza energię elektryczną i powoduje wysłanie telegramu radiowego zgodnego ze standardem Bluetooth Low Energy. Telegram przekazuje stan wszystkich czterech styków przyciskowych w chwili naciśnięcia albo zwolnienia listwy. Telegramy 03925 są zabezpieczone mechanizmem AES-128 opartym na indywidualnym kluczu prywatnym urządzenia. Rysunek 1: urządzenie 03925 (oryginał, strona 4).

1.2 Dane techniczne

Parametr	Wartość
Antena	Zintegrowana antena na płytce drukowanej
Zmierzona maksymalna moc nadawcza	0,4 dBm / 1,1 mW
Zasięg komunikacji - orientacyjny	75 m przy idealnej widoczności bez przeszkód / 10 m wewnątrz budynku
Standard komunikacji	Bluetooth Low Energy (BLE)
Częstotliwość radiowa, minimum / maksimum	2402 MHz / 2480 MHz
Domyślne kanały radiowe	CH 37 / 38 / 39: 2402 / 2426 / 2480 MHz
Zdarzenia rozgłoszeniowe na naciśnięcie lub zwolnienie, minimum / maksimum	2 / 3
Szybkość transmisji i modulacja	1 Mbit/s, GFSK
Interfejs konfiguracji	NFC Forum Type 2 Tag; ISO/IEC 14443, części 2 i 3
Identyfikacja urządzenia	Indywidualny 48-bitowy identyfikator urządzenia, programowany fabrycznie
Zabezpieczenie	AES128, tryb CBC, z kodem sekwencyjnym
Zasilanie	Wbudowany przetwornik energii kinetycznej
Wejścia przyciskowe	Do czterech przycisków lub dwóch klawiszy kołyskowych

1.3 Warunki środowiskowe

Parametr	Wartość
Temperatura pracy	Od -25 °C do +65 °C
Temperatura przechowywania	Od -25 °C do +65 °C
Wilgotność	0-95% wilgotności względnej, bez kondensacji

2. Informacje funkcjonalne

2.1 Przegląd urządzenia 03925

Moduł nadajnika przyciskowego 03925 umożliwia wykonanie bezprzewodowego sterowania bez baterii. Wysyła telegramy danych Bluetooth Low Energy (BLE), wykorzystując energię dostarczaną przez wbudowany generator elektrodynamiczny. Wygląd urządzenia pokazano na rysunku 2 (strona 5 oryginału).

Legenda rysunku 2: zatrzask i oś obrotu przycisków lub klawisza kołyskowego; (1) listwa generatora po obu stronach urządzenia; (2) styki przycisków służące do identyfikowania położenia klawisza. Podpis: moduł nadajnika przyciskowego 03925 z zasilaniem elektrodynamicznym.

2.2 Podstawowe działanie

Urządzenia 03925 zawierają elektrodynamiczny przetwornik energii uruchamiany listwą (1). Listwę naciska odpowiedni przycisk, klawisz kołyskowy lub podobny element zamontowany na urządzeniu. Wewnętrzna sprężyna zwalnia listwę, kiedy przestaje ona być naciskana.

Po naciśnięciu listwy wytwarzana jest energia elektryczna i wysyłany jest telegram BLE identyfikujący czynność (naciśnięcie albo brak naciśnięcia) oraz stan czterech styków przyciskowych (2). Zwolnienie listwy również wytwarza energię, wykorzystywaną do wysłania innego telegramu radiowego.

Można dzięki temu odróżnić telegramy wysłane przy naciśnięciu listwy od telegramów wysłanych przy jej zwolnieniu. Rozpoznając te typy telegramów i mierząc czas między naciśnięciem a zwolnieniem, można rozróżniać długie i krótkie naciśnięcia. Ułatwia to realizację takich funkcji jak ściemnianie lub sterowanie osłonami, w tym ustawianie lameli.

2.3 Interfejs użytkownika

Urządzenie 03925 ma cztery styki przycisków. Są podzielone na dwa kanały: A i B. Każdy kanał zawiera dwa styki oznaczone stanem O oraz I. Przy każdym naciśnięciu albo zwolnieniu listwy przesyłany jest stan wszystkich czterech styków, naciśnięty lub nienaciśnięty, wraz z indywidualnym 48-bitowym identyfikatorem urządzenia.

Rysunek 3 (strona 5): rozmieszczenie i oznaczenia styków. Channel oznacza kanał, State - stan. Oznaczenia A, B, O i I zachowano jak w oryginale; w późniejszych polach telegramu styki są zapisywane A0, A1, B0 i B1.

3. Transmisja telegramów

3.1 Parametry kanałów radiowych

03925 wysyła telegramy rozgłoszeniowe Bluetooth Low Energy (BLE) w paśmie 2,4 GHz, od 2402 MHz do 2480 MHz. Domyślnie korzysta z trzech kanałów rozgłoszeniowych BLE: 37, 38 i 39. Wysłanie telegramu na tych trzech kanałach jest nazywane zdarzeniem rozgłoszeniowym (Advertising Event).

Można korzystać także z innych kanałów w zakresie 2402-2480 MHz; patrz wybór kanałów w rozdziale 6.6.9 (odsyłacz w źródle: 6.7.9). Wartość początkowa mechanizmu wybielania danych jest ustalana następująco: dla kanałów BLE zgodnie ze specyfikacją, jako numer kanału radiowego; dla kanałów własnych jako różnica względem 2400 MHz, np. 3 dla 2403 MHz.

Tabela 1 - kanały radiowe obsługiwane przez 03925:

Kanał	Częstotliwość	Typ
37	2402 MHz	Rozgłoszeniowy BLE
0	2404 MHz	Danych BLE
1	2406 MHz	Danych BLE
...	...	...
10	2424 MHz	Danych BLE

Kanał	Częstotliwość	Typ
38	2426 MHz	Rozgłoszeniowy BLE
11	2428 MHz	Danych BLE
12	2430 MHz	Danych BLE
...	...	...
36	2478 MHz	Danych BLE
39	2480 MHz	Rozgłoszeniowy BLE
40	2403 MHz	Własny kanał radiowy
41	2405 MHz	Własny kanał radiowy
...	...	...
77	2477 MHz	Własny kanał radiowy
78	2479 MHz	Własny kanał radiowy

3.2 Domyślna sekwencja transmisji radiowej

W konfiguracji standardowej 03925 wysyła telegramy w zdarzeniach rozgłoszeniowych. Jedno zdarzenie polega na wysłaniu tego samego telegramu kolejno na wszystkich wybranych kanałach radiowych, domyślnie BLE 37, 38 i 39, z minimalnym odstępem między nimi.

Dla zwiększenia niezawodności urządzenie wysyła kilka zdarzeń, minimum dwa i maksimum trzy, dla każdego zadziałania wejścia przyciskowego. Rysunek 4 (strona 6): CH37, CH38, CH39; przerwa 20 ms; CH37, CH38, CH39; przerwa 20 ms; CH37, CH38, CH39.

3.3 Sekwencje transmisji definiowane przez użytkownika

W niektórych sytuacjach potrzebne może być wysyłanie telegramów na kanałach innych niż trzy kanały rozgłoszeniowe. 03925 umożliwia zatem wybranie kanałów używanych dla telegramów danych i telegramów uruchomieniowych. Obsługiwane są następujące tryby:

• Zarówno telegramy uruchomieniowe, jak i telegramy danych są wysyłane na kanałach rozgłoszeniowych w trzech zdarzeniach rozgłoszeniowych. To konfiguracja domyślna opisana w rozdziale 3.2.

• Telegramy uruchomieniowe są wysyłane na kanałach rozgłoszeniowych w trzech zdarzeniach, a telegramy danych w sekwencji zdefiniowanej przez użytkownika.

• Zarówno telegramy uruchomieniowe, jak i telegramy danych są wysyłane w sekwencji zdefiniowanej przez użytkownika.

Tryb wybiera się rejestrem CUSTOM_VARIANT interfejsu konfiguracji NFC, opisanym w rozdziale 6.6.8 (w źródle: 6.7.8). Urządzenie obsługuje sekwencję trzech kanałów, podobną do domyślnego zdarzenia, lecz z wyborem kanałów; sekwencję dwóch kanałów, z czterema powtórzeniami na dwóch kanałach; oraz sekwencję jednego kanału, z sześcioma transmisjami na jednym kanale. Szczegóły podano poniżej.

3.3.1 Sekwencja trzech kanałów

Sekwencja jest podobna do domyślnej. Różnica polega na tym, że kanały radiowe, domyślnie BLE 37, 38 i 39, wybiera się rejestrami CH_REG1, CH_REG2 i CH_REG3. Telegram jest wysyłany najpierw na kanale CH_REG1, bezpośrednio potem na CH_REG2 i następnie na CH_REG3. Cała sekwencja jest wysyłana łącznie trzy razy, z przerwami 20 ms między powtórzeniami. Rysunek 5 (strona 7) pokazuje te trzy grupy i dwie przerwy. Format rejestrów opisano w rozdziale 6.6.9 (w źródle: 6.7.9).

3.3.2 Sekwencja dwóch kanałów

W tej sekwencji pomija się transmisję na trzecim kanale wybranym przez CH_REG3 i zamiast tego dodaje jedno powtórzenie: łącznie cztery. Telegram jest wysyłany na kanale CH_REG1, a bezpośrednio potem na CH_REG2. Sekwencja powtarza się łącznie cztery razy, z przerwami 20 ms. Pokazuje ją rysunek 6 (strona 7): cztery pary CH_REG1/CH_REG2 i trzy przerwy. Format rejestrów opisano w rozdziale 6.6.9 (w źródle: 6.7.9).

3.3.3 Sekwencja jednego kanału

W tej sekwencji pomija się transmisje na drugim i trzecim kanale, wybieranymi odpowiednio przez CH_REG2 i CH_REG3. Wszystkie transmisje odbywają się na kanale CH_REG1. Telegram jest wysyłany na nim sześć razy, z przerwami 20 ms. Rysunek 7 (strona 7) pokazuje sześć transmisji CH_REG1 i pięć przerw. Format CH_REG1 opisano w rozdziale 6.6.9 (w źródle: 6.7.9).

4. Format telegramu

03925 wysyła telegramy radiowe Bluetooth Low Energy (BLE) w paśmie 2,4 GHz. Szczegółowych informacji o standardzie BLE należy szukać w odpowiednich specyfikacjach. Rysunek 8 (strona 8) przedstawia strukturę ramki BLE:

Pole	Zawartość / długość
Preambuła	0xAA, 1 bajt
Adres dostępu	0x8E89BED6, 4 bajty
Nagłówek	2 bajty
Adres źródłowy	6 bajtów
Dane użytkowe (Payload)	0-31 bajtów
Suma kontrolna	3 bajty

Zawartość pól opisano poniżej. Podpis rysunku 8 w oryginale brzmi „Domyślna sekwencja transmisji radiowej”, choć ilustracja pokazuje strukturę ramki.

4.1 Preambuła

Preambuła BLE ma długość 1 bajtu i oznacza początek ramki BLE. Jej wartość jest zawsze ustawiona na 0xAA.

4.2 Adres dostępu

4-bajtowy adres dostępu BLE identyfikuje typ telegramu. W ramkach rozgłoszeniowych ma zawsze wartość 0x8E89BED6.

4.3 Nagłówek

Nagłówek BLE określa niektóre parametry telegramu radiowego. Rysunek 9 (strona 8), od bitu 15 (MSb) do bitu 0 (LSb), ma następującą strukturę:

Pole	Liczba bitów	Wartość / znaczenie
Nieużywane (UNUSED)	2	00
Długość (LENGTH)	6	Łączna długość adresu i danych użytkowych
RX ADDR	1	0: nieużywane
TX ADDR	1	1: losowy

Pole	Liczba bitów	Wartość / znaczenie
Nieużywane (UNUSED)	2	00
Typ (TYPE)	4	0010: rozgłaszanie tylko nadawcze, ADV_NONCONN_IND

4.4 Adres źródłowy

6-bajtowy adres źródłowy BLE (adres MAC) jednoznacznie identyfikuje każde urządzenie 03925. Obsługiwane są dwa tryby: stałego adresu źródłowego (domyślny), w którym adres nie zmienia się, ale jego dolne 32 bity można konfigurować przez NFC; oraz prywatnego adresu rozwiązywalnego, konfigurowanego przez NFC, w którym adres zmienia się dla każdej transmisji.

Domyślnie stosowany jest stały adres źródłowy. Zgodnie z zapisem źródła tryb prywatnego adresu rozwiązywalnego wybiera się ustawieniem flagi Private Source Address w rejestrze Configuration na 0b0; odwołanie źródła wskazuje 6.7.7, odpowiadający opis rejestru jest w 6.6.7. Oba tryby opisano niżej. Uwaga do źródła: zapis o wartości 0b0 należy czytać łącznie z domyślnym trybem i dokumentacją rejestru; nie zmieniono go w przekładzie na inną wartość.

4.4.1 Tryb stałego adresu źródłowego

Domyślnie adres źródłowy pozostaje stały podczas normalnej pracy. Można go odczytywać i konfigurować przez NFC, zgodnie z rozdziałem 6. Górne 2 bajty identyfikują typ urządzenia i we wszystkich 03925 mają wartość 0xE215; tych bajtów nie można zmieniać. Dolne 4 bajty są indywidualnie przydzielone każdemu urządzeniu. Można je zmienić interfejsem NFC opisanym w rozdziale 6.6.3 (w źródle: 6.7.3).

Rysunek 10 (strona 8): identyfikator typu produktu 16 bitów, 0xE215, następnie indywidualny adres urządzenia 32 bity; kolejność od MSB do LSB.

4.4.2 Tryb prywatnego rozwiązywalnego adresu źródłowego

W niektórych zastosowaniach pożądana jest okresowa zmiana adresu źródłowego 03925, aby uniemożliwić śledzenie jego transmisji. Jednocześnie odbiornik musi nadal jednoznacznie rozpoznawać każde urządzenie. W tym celu można przez NFC skonfigurować losowe, prywatne adresy rozwiązywalne.

Ich używanie wymaga wspólnego klucza w 03925 i odbiorniku: Identity Resolution Key (IRK), czyli klucza rozwiązywania tożsamości. Urządzenie używa jako IRK swojego indywidualnego klucza losowego. Można go skonfigurować przez NFC, zgodnie z rozdziałem 6.

48-bitowe pole adresu dzieli się na dwa podpola. Pole prand zawiera liczbę losową, której dwa najbardziej znaczące bity, według tekstu źródła, mają wartość 0b10. Wartość prand zmienia się dla każdego wysyłanego telegramu, ale poszczególne zdarzenia rozgłoszeniowe przekazujące ten sam telegram (rozdział 3) używają tej samej wartości. Pole hash zawiera wartość weryfikacyjną wyznaczoną z prand za pomocą IRK.

Rysunek 11 (strona 9) przedstawia prand 24 bity, w tym 22 bity danych losowych i dwa bity oznaczone na rysunku jako 0 oraz 1, oraz hash 24 bity, w kolejności MSB-LSB. Uwaga do źródła: zapis 0b10 w tekście i widoczne 0, 1 na rysunku zachowano, nie rozstrzygając różnicy oznaczeń kolejności bitów.

Wartość prand szyfruje się kluczem IRK. Dolne 24 bity wyniku szyfrowania są używane jako hash. Połączenie 24-bitowego prand z 24-bitowym hash jest wysyłane jako 48-bitowy prywatny adres rozwiązywalny.

Odbiornik przechowuje listę IRK wszystkich przypisanych nadajników. Kiedy odbierze telegram z prywatnym adresem rozwiązywalnym, rozpoznawanym według źródła po najbardziej znaczących bitach 0b10, sam wylicza 24-bitowy hash z odebranego 24-bitowego prand, kolejno używając IRK każdego przypisanego urządzenia. Jeśli dany IRK daje hash zgodny z odebranym, odbiornik rozpoznał nadajnik.

W tym ujęciu IRK pełni rolę adresu urządzenia, natomiast prand i hash pozwalają wybrać właściwy IRK z całego zestawu kluczy. Rysunek 12 (strona 9) pokazuje nadajnik z IRK 128 bitów i polami prand/hash po 24 bity oraz odbiornik sprawdzający kolejno IRK urządzeń 1, 2, 3, ... n. Zgodny IRK określa tożsamość urządzenia.

4.5 Suma kontrolna

3-bajtowa suma kontrolna BLE służy do weryfikacji integralności odebranych telegramów. Jest obliczana jako CRC (cykliczny kod nadmiarowy) pól nagłówka BLE, adresu źródłowego i danych użytkowych.

4.6 Dane użytkowe (Payload)

Dane użytkowe telegramu danych mają 13-17 bajtów, zależnie od długości pola Optional Data, i składają się z poniższych pól:

Pole	Długość	Znaczenie
Length	1 bajt	Łączna długość kolejnych pól. Dla Optional Data o długości 0 / 1 / 2 / 4 bajty wynosi odpowiednio 12 / 13 / 14 / 16 bajtów, czyli 0x0C / 0x0D / 0x0E / 0x10
Type	1 bajt	Typ danych; dla telegramów danych 03925 zawsze 0xFF, dane właściwe dla producenta
Manufacturer ID	2 bajty	Identyfikator producenta BLE. Vimar przydzielono 0x03DA. Można go zmieniać przez NFC, opis w 6.6.5 (w źródle 6.7.5)
Sequence Counter	4 bajty	Stale zwiększany licznik używany w zabezpieczeniach. Fabrycznie 0, zwiększany przy każdym telegramie danych lub uruchomieniowym
Switch Status	1 bajt	Informacja o czynności przycisku; kodowanie w 4.7
Optional Data	0 / 1 / 2 / 4 bajty	Dodatkowe dane użytkownika w każdym telegramie, np. cechy właściwe dla danego zastosowania. Długość określa Configuration, opis w 6.6.7 (w źródle 6.7.7)
Security Signature	4 bajty	Podpis służący do uwierzytelniania telegramu, opis w 4.8

Rysunek 13 (strona 10): kolejno LEN 0x0C-0x10, TYPE 0xFF, Manufacturer ID 0x03DA, Sequence Counter 4 bajty, Switch Status, Optional Data 0/1/2/4 bajty i Security Signature 4 bajty.

4.7 Kodowanie stanu przycisków

Pole Switch Status identyfikuje czynność 03925: naciśnięcie albo zwolnienie. Urządzenie kolejno: 1) określa kierunek ruchu listwy, naciśnięcie albo zwolnienie; 2) odczytuje stan wejść wszystkich styków; 3) oblicza dane użytkowe; 4) oblicza podpis bezpieczeństwa.

Typ czynności wskazuje bit 0 (Energy Bar). Jeżeli podczas naciśnięcia lub zwolnienia dany styk został uruchomiony, odpowiadający mu bit stanu ma wartość 1. Wszystkie styki naciśnięte przy naciśnięciu listwy zostają zwolnione przy jej zwolnieniu. Mechanicznie niemożliwe jest dalsze przytrzymywanie jednego lub kilku styków podczas zwalniania listwy.

Rysunek 14 (strona 10) - kodowanie czynności:

Bity	Pole	Kodowanie
7, 6, 5	Zarezerwowane	Wymagane 0b000
4	B1	0: brak czynności; 1: czynność
3	B0	0: brak czynności; 1: czynność
2	A1	0: brak czynności; 1: czynność
1	A0	0: brak czynności; 1: czynność
0	Typ czynności	0: zwolnienie; 1: naciśnięcie

4.8 Uwierzytelnianie telegramów 03925

Uwierzytelnianie zapewnia przyjmowanie tylko telegramów od nadawców używających wcześniej wymienionego klucza bezpieczeństwa. Opiera się na 32-bitowym podpisie obliczanym według rysunku 15 (strona 11) i przesyłanym jako część telegramu.

Licznik sekwencji, adres źródłowy i pozostałe dane telegramu stanowią dane wejściowe algorytmu podpisu. Algorytm używa szyfrowania AES128 oraz indywidualnego losowego klucza bezpieczeństwa do wyznaczenia 32-bitowego podpisu wysyłanego w telegramie. Podpis zależy zatem od aktualnego licznika, adresu źródłowego i danych użytkowych; zmiana dowolnego z tych trzech parametrów zmienia podpis.

Odbiornik wykonuje te same obliczenia z licznika, adresu i pozostałych danych odebranego telegramu, używając klucza otrzymanego od 03925 podczas uruchomienia. Następnie porównuje podpis odebrany z obliczonym. Ich zgodność potwierdza, że nadawca i odbiornik używają tego samego klucza oraz że treść wiadomości - adres, licznik i dane - nie została zmieniona. Odbiornik potwierdził w ten sposób pochodzenie z zaufanego nadajnika identyfikowanego kluczem i poprawność treści.

Aby zapobiec przechwyceniu i ponownemu wysłaniu prawidłowej wiadomości (atakowi replay), odbiornik musi śledzić licznik 03925 i akceptować tylko telegramy z wartościami większymi. Dla następnych telegramów nie wolno przyjmować wartości równych ani mniejszych. Legenda rysunku 15: telegram radiowy - licznik sekwencji, adres źródłowy, dane telegramu, podpis 32 bity; AES128; klucz bezpieczeństwa 128 bitów.

4.8.1 Implementacja uwierzytelniania

03925 uwierzytelnia telegramy za pomocą AES128 w trybie CCM (Counter with CBC-MAC), opisanym w IETF RFC3610. W chwili sporządzenia instrukcji specyfikacja była dostępna pod adresem https://www.ietf.org/rfc/rfc3610.txt.

13-bajtowa wartość inicjalizacyjna CCM Nonce, używana tylko raz i unikalna, jest połączeniem 6-bajtowego adresu źródłowego, 4-bajtowego licznika sekwencji i trzech bajtów 0x00 jako dopełnienia. Adres i licznik używają kolejności little endian: najmniej znaczący bajt jako pierwszy.

Rysunek 16 (strona 11): AES128 Nonce, 13 bajtów; adres źródłowy bajty 0-5, licznik sekwencji bajty 0-3, dopełnienie 0x00, 0x00, 0x00. Nonce i indywidualny 128-bitowy klucz służą do wyliczenia 32-bitowego podpisu uwierzytelnianych danych użytkowych.

Rysunek 17 (strona 11): uwierzytelniane dane to LEN bajt 0, TYPE 0xFF, MANUFACTURER 0x03DA, licznik sekwencji bajty 0-3, STATE bajt 0, Optional Data 0/1/2/4 bajty. Obliczony 32-bitowy podpis jest dopisywany do danych użytkowych telegramu zgodnie z rysunkiem 13 w rozdziale 4.6.

5. Uruchomienie

Uruchomienie oznacza przypisanie 03925 do odbiornika, np. modułu wykonawczego, sterownika lub bramki. Obejmuje dwa zadania: identyfikację urządzenia i wymianę parametrów zabezpieczeń.

Odbiornik musi wiedzieć, jak jednoznacznie rozpoznać konkretne 03925. Zapewnia to indywidualny 48-bitowy identyfikator, adres źródłowy z rozdziału 4.4. Dodatkowo można skonfigurować do 4 bajtów Optional Data, zgodnie z rozdziałem 6.6.6 (odwołanie źródła: 6.7.6).

Odbiornik musi także uwierzytelniać telegramy, aby mieć pewność, że pochodzą z danego urządzenia i nie zostały zmienione (4.8). W tym celu wymieniany jest 128-bitowy losowy klucz używany przez 03925 do uwierzytelniania telegramów.

Urządzenie udostępnia trzy sposoby. Przy uruchomieniu przez NFC parametry odczytuje odpowiednie narzędzie, np. smartfon NFC z właściwym oprogramowaniem, będący już częścią sieci docelowej. Narzędzie przekazuje je zamierzonemu odbiornikowi; interfejs NFC opisano w rozdziale 6. Przy uruchomieniu aparatem kod Data Matrix (DMC) modułu identyfikuje urządzenie i klucz. Narzędzie, np. smartfon będący już częścią sieci, odczytuje kod i przekazuje parametry odbiornikowi. Przy uruchomieniu radiowym specjalne telegramy przekazują parametry bezpośrednio odbiornikowi; urządzenie przełącza się w tym celu tymczasowo w tryb opisany w 5.3.

5.1 Uruchomienie przez NFC

Wszystkie wymagane parametry można odczytać czytnikiem/zapisującym NFC zgodnym z ISO/IEC 14443, części 2 i 3. W 03925 zastosowano znacznik Mifare Ultralight. Należy wykonać następujące czynności:

1. Odblokuj urządzenie domyślnym kodem NFC PIN 0x0000E215.

2. Odczytaj adres źródłowy, klucz bezpieczeństwa i licznik sekwencji 03925, a następnie odpowiednio skonfiguruj odbiornik.

3. WAŻNE: fabryczny losowy klucz można uzyskać z kodu DMC (5.2), odebranych telegramów uruchomieniowych (5.3) i interfejsu NFC. W zastosowaniach istotnych dla bezpieczeństwa, gdy osoby nieuprawnione mogą mieć fizyczny dostęp do przycisku, zdecydowanie zaleca się zmianę klucza na nowy podczas uruchomienia przez NFC, według procedury 6.6.4 (w źródle: 6.7.4). Dodatkowo można zablokować odczyt nowego klucza przez NFC, ustawiając flagę Private Security Key w rejestrze Configuration przed jego zapisaniem. Wtedy nawet osoba znająca poprawny PIN nie odczyta nowego klucza. Nowy klucz należy prawidłowo udokumentować: po takim zapisaniu nie ma możliwości jego odzyskania.

4. WAŻNE: po zaprogramowaniu nowego klucza zdecydowanie zaleca się wyłączenie uruchamiania radiowego. Uniemożliwia to odczyt klucza przez wyzwolenie telegramu uruchomieniowego, jak w 5.3. Ustaw flagę Disable Radio Commissioning na 0b1; opis w 6.6.7 (w źródle: 6.7.7).

5. WAŻNE: zawsze zmień domyślny PIN NFC na nowy i zablokuj interfejs konfiguracji NFC. Ten krok jest obowiązkowy, aby uniemożliwić dostęp za pomocą domyślnego kodu. Po utracie nowego PIN można wykonać reset fabryczny i odzyskać domyślny PIN (5.4; źródło błędnie odsyła do rozdziału 0). Ze względów bezpieczeństwa reset zawsze przywraca również fabryczny klucz bezpieczeństwa.

5.2 Uruchomienie z użyciem aparatu

Każdy moduł ma optycznie odczytywany kod uruchomieniowy w postaci Data Matrix albo QR, zależnie od wersji urządzenia. Kod na etykiecie można zeskanować odpowiednim narzędziem, np. smartfonem lub komputerem z czytnikiem DMC/QR, aby odczytać stały adres źródłowy i klucz bezpieczeństwa. Narzędzie może wykorzystać te dane do skonfigurowania odbiornika telegramów 03925.

5.3 Uruchomienie radiowe

Gdy NFC i aparat nie mogą być wykorzystane, można włączyć specjalny tryb wysyłania telegramów uruchomieniowych. Funkcję tę można wyłączyć przez NFC, ustawiając Disable Radio Commissioning w Configuration na 0b1; patrz 6.6.7 (w źródle: 6.7.7).

5.3.1 Wejście w tryb uruchamiania

Wykorzystuje się specjalną sekwencję styków, pokazaną na rysunku 18 (strona 13). Najpierw wybierz dowolny styk: A0, A1, B0 albo B1. Jest on dalej oznaczany Button_X. Wykonaj sekwencję długie-krótkie-długie:

1. Naciśnij wybrany przycisk razem z listwą generatora, przytrzymaj ponad 7 sekund, a następnie zwolnij.

2. Naciśnij ten sam przycisk razem z listwą krótko, na mniej niż 2 sekundy.

3. Ponownie naciśnij ten sam przycisk wraz z listwą, przytrzymaj ponad 7 sekund i zwolnij.

Po rozpoznaniu sekwencji 03925 przejdzie w tryb uruchamiania, jeżeli Disable Radio Commissioning w Configuration interfejsu NFC ma wartość 0b0, czyli ustawienie domyślne. Legenda rysunku 18: tryb normalny (domyślny), sekwencja długie + krótkie + długie Button_X, tryb uruchamiania, krótki Button_X, dowolna inna czynność przycisku; każda inna sekwencja pozostawia tryb normalny.

5.3.2 Wysyłanie telegramu uruchomieniowego

Po wejściu w ten tryb urządzenie wysyła telegram uruchomieniowy na kanałach wybranych jak w 3.1. Następne telegramy uruchomieniowe są wysyłane przy każdym ponownym naciśnięciu lub zwolnieniu przycisku użytego do wejścia w tryb, Button_X.

Dane użytkowe telegramu uruchomieniowego mają 30 bajtów:

Pole	Długość	Znaczenie
Length	1 bajt	Zawsze 0x1D: 29 bajtów dalszych danych właściwych dla producenta
Type	1 bajt	0xFF: dane właściwe dla producenta
Manufacturer ID	2 bajty	Domyślnie 0x03DA; w tej części źródła dopisano „GmbH”. Możliwa zmiana przez NFC, 6.6.5 (w źródle: 6.7.5)
Sequence Counter	4 bajty	Fabrycznie 0, zwiększany z każdym wysłanym telegramem danych lub uruchomieniowym
Security Key	16 bajtów	Indywidualny losowy klucz, generowany i programowany podczas produkcji. Przesyłany przy uruchomieniu, aby odbiornik mógł uwierzytelniać dane
Static Source Address	6 bajtów	Jednoznaczny identyfikator urządzenia BLE. Oprócz adresu ramki (4.4.1) powtarzany w danych użytkowych, ponieważ niektóre urządzenia, zwłaszcza z iOS według źródła, nie udostępniają adresu ramki aplikacjom; bez tego przypisanie w takich aplikacjach nie byłoby możliwe

Rysunek 19 (strona 13): LEN 0x1D; TYP 0xFF; Manufacturer ID 0x03DA; dane producenta: licznik 4 bajty, klucz 16 bajtów, stały adres źródłowy 6 bajtów.

5.3.3 Wyjście z trybu uruchamiania

Naciśnięcie dowolnego przycisku innego niż Button_X przerywa wysyłanie telegramów uruchomieniowych i przywraca zwykłą transmisję telegramów danych.

5.4 Przywracanie ustawień fabrycznych

Reset przywraca domyślne ustawienia, co pozwala odzyskać znaną konfigurację po utracie PIN NFC lub gdy dostęp przez NFC nie jest możliwy z innych przyczyn. Zdejmij klawisz lub klawisze i obudowę przycisku z modułu. Naciśnij jednocześnie wszystkie cztery styki A0, A1, B0, B1 i wciśnij listwę generatora.

Listwa musi pozostać wciśnięta przez co najmniej 10 sekund przed zwolnieniem. Styki A0, A1, B0, B1 można zwolnić w dowolnym momencie po naciśnięciu listwy; nie trzeba trzymać ich przez 10 sekund.

Po rozpoznaniu czynności urządzenie przywraca: stały adres źródłowy; Security Key i Security Key Write, oba do fabrycznego klucza; Manufacturer ID do 0x03DA, z dopiskiem „GmbH” w źródle; NFC PIN do 0x0000E215. Adres źródłowy i klucz ponownie odpowiadają kodowi DMC na etykiecie. Dodatkowo Configuration i Custom Variant są zerowane do 0x00.

6. Interfejs NFC

03925 realizuje funkcję NFC Forum Type 2 Tag zgodną z ISO/IEC 14443, części 2 i 3, przy użyciu znacznika NXP NT3H2111 Mifare Ultralight. Funkcjonalność NFC pozwala odczytywać i zapisywać pamięć konfiguracji urządzenia, a przez to konfigurować je zgodnie z poniższym opisem. Rozdział 6.1 wprowadza funkcje i sposoby używania interfejsu. Szczegółowej pomocy przy integrowaniu NFC NXP NT3H2111 z oprogramowaniem komputera lub smartfona udziela wsparcie techniczne NXP.

6.1 Korzystanie z interfejsu NFC

Potrzebne są: czytnik NFC, jako akcesorium USB do komputera albo odpowiedni smartfon/tablet, oraz oprogramowanie NFC z funkcjami odczytu, zapisu, blokowania PIN, odblokowania PIN i zmiany PIN.

6.2 Funkcje interfejsu NFC

Szczegółowy opis funkcji zawiera norma ISO/IEC 14443. Zagadnienia właściwe dla implementacji NXP NT3H2111 opisano w dokumentacji NXP, dostępnej w chwili sporządzania instrukcji pod adresem http://cache.nxp.com/documents/data_sheet/NT3H2111_2211.pdf. Dalsze punkty zestawiają funkcje do celów referencyjnych.

6.2.1 Automat stanów interfejsu NFC

Rysunek 20 (strona 15 oryginału) pokazuje pełny automat stanów. Nazwy stanów i poleceń są identyfikatorami protokołu i pozostają po angielsku. POR to reset po włączeniu zasilania. IDLE oznacza oczekiwanie; HALT - zatrzymanie; READY 1 i READY 2 - kolejne etapy identyfikacji; ACTIVE - stan aktywny; AUTHENTICATED - stan po uwierzytelnieniu.

Procedura identyfikacji i wyboru obejmuje REQA / WUPA, ANTICOLLISION, SELECT cascade level 1 i SELECT cascade level 2. HLTA prowadzi do HALT, a WUPA umożliwia ponowne wybudzenie. PWD_AUTH przenosi ze stanu ACTIVE do AUTHENTICATED. Przy stanach ACTIVE i AUTHENTICATED rysunek wymienia operacje pamięci READ, FAST_READ, WRITE, GET_VERSION i READ_SIGN; przy ACTIVE widnieje ponadto FAST_WRITE, przy AUTHENTICATED ponownie PWD_AUTH. Pełne strzałki automatu zachowano w dołączonym oryginale.

6.2.2 Stan IDLE

IDLE jest stanem oczekiwania po resecie po włączeniu zasilania (POR), czyli po wprowadzeniu znacznika NFC w pole magnetyczne czytnika. Znacznik przechodzi z IDLE do READY 1 po odebraniu REQA albo WUPA. Czytnik wysyła te polecenia, aby wykryć obecność kart w swoim zasięgu. Inne dane odebrane w IDLE są odrzucane i znacznik pozostaje w tym stanie.

6.2.3 Stan READY 1

To pierwszy etap rozpoznawania UID: znacznik ustala pierwsze 3 bajty 7-bajtowego UID, korzystając z ANTICOLLISION lub SELECT poziomu kaskadowego 1. Po wykonaniu SELECT poziomu 1 z dopasowaną, pełną pierwszą częścią UID wychodzi z READY 1 i przechodzi do READY 2, w którym rozpoznaje drugą część UID.

6.2.4 Stan READY 2

To drugi etap rozpoznawania UID: znacznik ustala pozostałe 4 bajty 7-bajtowego UID za pomocą ANTICOLLISION lub SELECT poziomu kaskadowego 2. Po wykonaniu SELECT poziomu 2 z dopasowaną pełną częścią UID wychodzi z READY 2 i przechodzi do ACTIVE, w którym można wykonywać polecenia związane z aplikacją.

6.2.5 Stan ACTIVE

Stan ACTIVE umożliwia odczyt i zapis pamięci niechronionej. Gdy wymagany jest dostęp do pamięci chronionej, znacznik może przejść do AUTHENTICATED po wykonaniu PWD_AUTH z poprawnym 32-bitowym hasłem.

6.2.6 Polecenie odczytu

READ wymaga adresu strony początkowej i zwraca 16 bajtów z czterech stron znacznika, po 4 bajty na stronę. Przykładowo adres 03h zwraca strony 03h, 04h, 05h i 06h. Gdy adres READ znajduje się blisko końca dostępnej pamięci, obowiązują warunki szczególne.

Rysunek 21 (strona 16) pokazuje sekwencję odczytu: czytnik NFC wysyła Cmd (polecenie), Addr (adres), CRC; znacznik NFC odpowiada Data (dane) i CRC w przypadku ACK, czyli potwierdzenia, albo NAK, czyli odpowiedzi odmownej. Czas polecenia: 368 µs; odpowiedzi danych: 1548 µs; odpowiedzi NAK: 57 µs. TACK i TNAK oznaczają pokazane na schemacie czasy oczekiwania na odpowiedź.

6.2.7 Polecenie zapisu

WRITE wymaga adresu strony początkowej i zapisuje na tej stronie 4 bajty danych. Rysunek 22 (strona 16) przedstawia sekwencję zapisu; w podpisie źródłowym omyłkowo nazwano ją sekwencją odczytu.

Czytnik wysyła Cmd, Addr, Data i CRC; czas tej transmisji wynosi 708 µs. Znacznik odpowiada ACK po TACK albo NAK po TNAK. Każda z tych odpowiedzi ma na schemacie czas 57 µs. Identyfikatory poleceń i zależności czasowe przedstawiono bez zmian w oryginale.

6.2.8 Polecenie uwierzytelnienia hasłem (PWD_AUTH)

Do chronionego obszaru pamięci można uzyskać dostęp tylko po poprawnej weryfikacji hasła za pomocą PWD_AUTH. Polecenie przyjmuje hasło jako parametr, a po sukcesie zwraca PACK, czyli potwierdzenie uwierzytelnienia hasła.

Rysunek 23 (strona 17): czytnik NFC wysyła Cmd, Pwd (hasło), CRC w czasie 623 µs. Znacznik odpowiada PACK i CRC po TACK, z czasem odpowiedzi 368 µs, albo NAK po TNAK, z czasem 57 µs.

Po poprawnym uwierzytelnieniu można zmienić hasło, zapisując nowe na stronie pamięci 0xE5. Odczyt strony 0xE5 zawsze zwraca 0x00000000: bieżącego kodu PIN nie można odczytać.

6.3 Organizacja pamięci konfiguracji

Pamięć konfiguracji 03925 jest podzielona na dane publiczne i dane chronione. Oprócz tego urządzenie utrzymuje prywatny obszar konfiguracji na parametry domyślne i informacje poufne, niedostępny dla użytkownika. Rysunek 24 (strona 17) przedstawia organizację pamięci:

Obszar	Zawartość	NFC bez PIN	NFC z PIN
Dane publiczne (Public Data)	Nazwa produktu PTM 215B; Product ID; Manufacturer ID; Source Address; Sequence Counter; wersje HW / SW / NFC	Tylko odczyt	Tylko odczyt
Dane chronione, na rysunku Product Data	Source Address Write; Manufacturer ID Write; Product ID Write; Security Key Write; Optional Data; Configuration; Custom Variant; Custom Radio Channel; Custom NFC Data	Brak dostępu	Odczyt / zapis
Dane prywatne (Private Data)	Security Key; ustawienia domyślne	Brak dostępu	Brak dostępu

6.4 Mapa adresów pamięci

Dostępna przez NFC pamięć konfiguracji jest zorganizowana w strony po 4 bajty. Odczyt NFC zwraca 16 bajtów, czyli 4 strony, a zapis obejmuje 4 bajty, czyli jedną stronę. Kolejność bajtów jest little endian: najpierw odczytywany jest bajt 0, na końcu bajt 3. Tabela 2 (strona 18) określa poniższą mapę; bajt 0 to LSB, bajt 3 to MSB.

Obszar	Strony NFC	Przesunięcie bajtowe	Zawartość
Publiczny	0 (0x00) ... 3 (0x03)	0 ... 12	Zarezerwowane
Publiczny	4 (0x04), 5 (0x05)	16, 20	Nazwa produktu PTM 215B
Publiczny	6 (0x06), 7 (0x07)	24, 28	Product ID
Publiczny	8 (0x08)	32	Bajty 0-1: NFC Revision; bajty 2-3: Manufacturer ID
Publiczny	9 (0x09)	36	Zarezerwowane
Publiczny	10 (0x0A)	40	Hardware Revision
Publiczny	11 (0x0B)	44	Software Revision
Publiczny	12 (0x0C)	48	Static Source Address
Publiczny	13 (0x0D)	52	Sequence Counter

Obszar	Strony NFC	Przesunięcie bajtowe	Zawartość
Chroniony	14 (0x0E)	56	Bajt 0: Configuration; bajt 1: Variant; bajty 2-3: zarezerwowane
Chroniony	15 (0x0F)	60	Bajty 0-3: Opt Data 0, 1, 2, 3
Chroniony	16 (0x10), 17 (0x11)	64, 68	Product ID Write
Chroniony	18 (0x12)	72	Source ID Write
Chroniony	19 (0x13)	76	Bajty 0-1: Manufacturer ID Write; bajty 2-3: zarezerwowane
Chroniony	20 (0x14) ... 23 (0x17)	80 ... 92	Security Key Write
Chroniony	24 (0x18)	96	Bajt 0: CH_REG1; bajt 1: CH_REG2; bajt 2: CH_REG3; bajt 3: zarezerwowany
Chroniony	25 (0x19) ... 31 (0x1F)	100 ... 124	Zarezerwowane
Chroniony	32 (0x20) ... 95 (0x5F)	128 ... 380	Customer NFC Data
Chroniony	96 (0x60) ... 225 (0x10) [zapis źródła]	384 ... 900	Zarezerwowane
Chroniony	229 (0xE5)	916	PIN Code, tylko zapis

Uwaga do tabeli źródłowej: przy stronie dziesiętnej 225 podano 0x10. Jest to niespójne z zapisem dziesiętnym i przesunięciem 900; zachowano oznaczenie źródłowe zamiast podawać je jako zweryfikowany adres. Przy pracy z pamięcią należy posłużyć się dokumentacją znacznika i aktualnymi danymi producenta.

6.5 Dane publiczne

Dane publiczne może odczytać każde urządzenie NFC obsługujące ISO/IEC 14443, części 2 i 3. Nie stosuje się szczególnych środków ograniczających ten odczyt. Obszar zawiera:

• Nazwę produktu 03925: zawsze PTM 215B.

• Product ID: pole 8-bajtowe, domyślnie 0x0000000000000000. Product ID i Manufacturer ID mogą być skonfigurowane przez użytkownika do identyfikowania produktu opartego na 03925; opis w 6.6.5.

• Manufacturer ID: pole 2-bajtowe identyfikujące producenta BLE (4.6), domyślnie 0x03DA, z dopiskiem „GmbH” w tej części źródła. Możliwa konfiguracja razem z Product ID według 6.6.5.

• Static Source Address: pole 4-bajtowe identyfikujące stały adres z 4.4.1. Każdy egzemplarz ma indywidualny fabryczny adres. Użytkownik może go zmienić w celu identyfikacji swojego produktu, zgodnie z 6.6.3.

• Hardware Revision, Software Revision i NFC Revision: pola identyfikujące wersje urządzenia.

• Telegram Sequence Counter: 4-bajtowy licznik fabrycznie ustawiony na 0 i zwiększany przy każdym wysłanym telegramie. Aby zapobiegać atakom replay, odbiorniki nigdy nie powinny przyjmować telegramów z licznikiem równym lub mniejszym od poprzednio odebranego.

Zmiany Static Source Address, Manufacturer ID i Product ID są możliwe tylko przez chroniony dostęp opisany niżej, co chroni je przed nieuprawnioną modyfikacją. Ze względów bezpieczeństwa licznika sekwencji telegramów nie można zapisać ani wyzerować żadnym mechanizmem.

6.6 Dane chronione

Obszar chroniony zawiera następujące elementy:

Rejestr	Opis
Source Address Write	4 bajty do aktualizacji dolnych 4 bajtów Static Source Address; 6.6.3
Product ID Write	8 bajtów do aktualizacji Product ID; 6.6.5
Manufacturer ID Write	Według wykazu źródła rejestr 4-bajtowy, do aktualizacji Manufacturer ID; 6.6.5. Sam identyfikator ma 2 bajty; pozostałe 2 są w mapie zarezerwowane
Security Key Write	16 bajtów do aktualizacji klucza bezpieczeństwa; 6.6.4
Optional Data	4 bajty danych opcjonalnych wysyłanych w telegramach (4.6). Najpierw Optional Data 0, na końcu Optional Data 3
Configuration	1 bajt konfigurujący funkcjonalne zachowanie urządzenia; 6.6.7
Custom Variant	1 bajt konfigurujący zachowanie transmisji; 6.6.8
Custom Radio Channel: CH_REG1, CH_REG2, CH_REG3	Rejestry po 1 bajcie, wybierające kanały w niestandardowym trybie transmisji; 6.6.9
Custom NFC Data	Wykaz źródła podaje rezerwację 64 bajtów danych użytkownika i odsyła do 6.6.10. Uwaga: 6.6.10 oraz mapa stron podają 64 strony, czyli 256 bajtów; ta rozbieżność pochodzi z oryginału

6.6.1 Kod PIN

Dostęp do danych chronionych wymaga odblokowania pamięci konfiguracji poprawnym 32-bitowym PIN. Domyślnie obszar jest zablokowany, a kod odblokowujący wynosi 0x0000E215.

Podczas instalacji domyślny PIN należy zmienić na własny. Odblokuj NFC starym kodem i zapisz nowy na stronie 0xE5. Źródło odsyła w tym miejscu do 6.3.1; procedurę uwierzytelnienia i zmiany hasła opisano faktycznie w 6.2.8.

6.6.2 Konfiguracja parametrów produktu

03925 nie pozwala bezpośrednio zmieniać Static Source Address, Product ID, Manufacturer ID ani Security Key. Nową wartość należy najpierw zapisać w odpowiednim rejestrze obszaru chronionego: Source Address Write, Product ID Write, Manufacturer ID Write albo Security Key Write, a następnie ustawić odpowiadającą jej flagę Update w Configuration. Po tym trzeba nacisnąć i zwolnić listwę generatora modułu.

6.6.3 Rejestr Source Address Write

Rejestr ma 4 bajty i pozwala zmienić dolne 32 bity stałego adresu źródłowego. Górne 16 bitów są zawsze ustalone na 0xE215, aby identyfikować typ urządzenia. Aby zmienić dolne 32 bity:

1. Zapisz nowy adres w Source Address Write.

2. Ustaw Update Source Address w Configuration na 0b1.

3. Naciśnij i zwolnij listwę generatora 03925.

Urządzenie rozpozna żądanie zmiany na podstawie flagi i skopiuje Source Address Write do dolnych 32 bitów Source Address. Po poprawnym wykonaniu zeruje flagę Update Source Address do 0b0.

6.6.4 Rejestr Security Key Write

16-bajtowy rejestr zawiera indywidualny losowy klucz bezpieczeństwa. Fabryczny klucz można zastąpić własnym następująco:

1. Zapisz nowy klucz w Security Key Write. Ze względów bezpieczeństwa nie można ustawić klucza na 0x00000000000000000000000000000000 ani 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF. Zapisanie jednej z tych wartości nie powoduje aktualizacji klucza.

2. Ustaw Update Security Key w Configuration na 0b1.

3. Jeżeli klucz ma być tylko zapisywalny, bez możliwości odczytu po aktualizacji, ustaw Private Security Key w Configuration na 0b1.

4. Naciśnij i zwolnij listwę generatora.

Urządzenie rozpozna flagę Update Security Key i skopiuje Security Key Write do Security Key w pamięci prywatnej. Po poprawnym wykonaniu ustawi Update Security Key na 0b0.

Jeśli Private Key w Configuration ma wartość 0b0, zawartość Security Key Write pozostaje niezmieniona. Pozwala to odczytywać klucz użytkownikom znającym poprawny PIN. Jeśli Private Key ma wartość 0b1, po poprawnym wykonaniu Security Key Write zostaje wyzerowany do 0x00000000000000000000000000000000. Zapewnia to brak możliwości odczytu klucza nawet osobom znającym PIN.

Security Key Write pozostanie wyzerowany również po późniejszym przestawieniu Private Key na 0b0. Nie można dzięki temu odczytać klucza zapisanego przy ustawionej fladze Private Key.

Jeżeli Security Key Write zostanie przypadkowo nadpisany lub wyczyszczony przez NFC, nie będzie możliwy odczyt aktualnego klucza przez NFC. Wtedy trzeba zapisać nowy klucz według tej procedury albo przywrócić fabryczny klucz przez reset. Pamięć chroniona jest przeznaczona do obsługi 1000 zmian klucza bezpieczeństwa.

6.6.5 Rejestry Product ID Write i Manufacturer ID Write

Product ID ma 8 bajtów i pozwala określić publicznie dostępny parametr, np. własny identyfikator lub nazwę. Narzędzie uruchomieniowe NFC może go odczytać do określenia typu produktu. Manufacturer ID ma 2 bajty, identyfikuje producenta produktu BLE i jest przesyłany w każdym telegramie. Domyślnie wynosi 0x03DA, z dopiskiem „GmbH” w źródle, ale można ustawić inny identyfikator OEM.

Zmiana identyfikatorów przebiega następująco:

1. Zapisz wymagany Product ID, 8 bajtów w kodowaniu HEX albo ASCII według wyboru użytkownika, w Product ID Write. Wartość 0x0000000000000000 oznacza, że Product ID nie zostanie zaktualizowany.

2. Zapisz wymagany Manufacturer ID, 2 bajty, w Manufacturer ID Write. Wartość 0x0000 oznacza brak aktualizacji Manufacturer ID.

3. Ustaw Update Product and Manufacturer ID w Configuration na 0b1.

4. Naciśnij i zwolnij listwę generatora.

Urządzenie rozpozna żądanie na podstawie flagi. Skopiuje każdą niezerową wartość Product ID Write do Product ID oraz każdą niezerową wartość Manufacturer ID Write do Manufacturer ID. Następnie wyzeruje Update Product and Manufacturer ID do 0b0.

6.6.6 Rejestr Optional Data

Rejestr pozwala określić do 4 bajtów własnych danych, przesyłanych w każdym telegramie danych. Mogą zawierać informacje właściwe dla użytkownika lub aplikacji. Długość Optional Data określa Configuration: 0 bajtów, czyli pole nieobecne i ustawienie domyślne, albo 1, 2 lub 4 bajty.

Gdy długość w Configuration jest niezerowa, 03925 odczytuje odpowiednią liczbę bajtów z Optional Data, zaczynając od najmniej znaczącego bajtu: bajtu 0, Optional Data 0. Dodatkowe dane wymagają większej energii transmisji radiowej i mogą zmniejszyć łączną liczbę nadmiarowo wysyłanych telegramów.

6.6.7 Rejestr Configuration

Rejestr ma 1 bajt i zawiera flagi konfiguracji. Rysunek 25 (strona 20) przedstawia następującą strukturę:

Bity	Flaga / pole	Znaczenie
7-6	Optional Data Field Size	0b00: wyłączone; 0b01: 1 bajt; 0b10: 2 bajty; 0b11: 4 bajty
5	Radio Commissioning Disable	Wyłączenie uruchamiania radiowego

Bity	Flaga / pole	Znaczenie
4	Source Address Private	Prywatny adres źródłowy
3	Security Key Private	Klucz prywatny, ograniczenie odczytu
2	Security Key Update	Aktualizacja klucza bezpieczeństwa
1	Product ID + Manufacturer ID Update	Aktualizacja identyfikatora produktu i producenta
0	Source Address Update	Aktualizacja adresu źródłowego

Wartości i procedury ustawiania flag opisano w odpowiednich punktach instrukcji. Sam rysunek nie podaje wartości logicznych włączających każdą z flag; nie dopisano ich na podstawie domysłu.

6.6.8 Rejestr Custom Variant

Rejestr ma 1 bajt i wybiera niestandardowy tryb transmisji z rozdziału 3.3. Tabela 3 (strona 21) zawiera następujące ustawienia:

Wartość	Znaczenie
0x00	Telegramy uruchomieniowe i danych w standardowym trybie rozgłoszeniowym, domyślnie. Odpowiada 0x04 z kanałami BLE CH37, CH38, CH39
0x01	Telegramy uruchomieniowe w standardowym trybie rozgłoszeniowym; dane na 3 kanałach użytkownika
0x02	Telegramy uruchomieniowe w standardowym trybie rozgłoszeniowym; dane na 2 kanałach użytkownika
0x03	Telegramy uruchomieniowe w standardowym trybie rozgłoszeniowym; dane na 1 kanale użytkownika
0x04	Telegramy uruchomieniowe i danych na 3 kanałach użytkownika
0x05	Telegramy uruchomieniowe i danych na 2 kanałach użytkownika
0x06	Telegramy uruchomieniowe i danych na 1 kanale użytkownika
0x07-0xFF	Nieużywane; traktowane jak 0x00

6.6.9 Rejestry wyboru kanału radiowego

Gdy Custom Variant ma wartość inną niż 0x00, kanały wybiera się za pomocą CH_REG1, CH_REG2 i CH_REG3 zgodnie z 3.3. Każdy rejestr ma 1 bajt i korzysta z kodowania tabeli 4. Dostępne są standardowe kanały BLE 0-39 na parzystych częstotliwościach 2402-2480 MHz oraz własne kanały pomiędzy kanałami standardowymi, na nieparzystych częstotliwościach 2403-2479 MHz.

Tabela 4 - wartości rejestru CH_REGn:

Wartość CH_REGn	Częstotliwość	Typ kanału
37	2402 MHz	Rozgłoszeniowy BLE
0	2404 MHz	Danych BLE

Wartość CH_REGn	Częstotliwość	Typ kanału
1	2406 MHz	Danych BLE
...	...	...
10	2424 MHz	Danych BLE
38	2426 MHz	Rozgłoszeniowy BLE
11	2428 MHz	Danych BLE
12	2430 MHz	Danych BLE
...	...	...
36	2478 MHz	Danych BLE
39	2480 MHz	Rozgłoszeniowy BLE
40	2403 MHz	Własny
41	2405 MHz	Własny
...	...	...
77	2477 MHz	Własny
78	2479 MHz	Własny

6.6.10 Dane użytkownika (Customer Data)

03925 przeznacza 64 strony, czyli 256 bajtów, na dane użytkownika odczytywane i zapisywane przez NFC w trybie chronionym. Głównym przeznaczeniem jest przechowywanie informacji OEM, np. typu produktu, wersji, kodu daty itp. Nie ma jednak ograniczeń rodzaju treści poza maksymalną długością 256 bajtów.

Urządzenie nie odczytuje ani nie modyfikuje tego obszaru. Jego zawartość nie jest zmieniana przez reset fabryczny. Oznacza to, że po resecie można ją odczytać przy użyciu domyślnego PIN. Dlatego nie wolno wykorzystywać tego obszaru do przechowywania danych wrażliwych.

6.7 Dane prywatne

Obszar prywatny przechowuje Security Key i ustawienia domyślne. Jego zawartość nie jest dostępna z zewnątrz.

6.7.1 Klucz bezpieczeństwa

Pole Security Key zawiera 128-bitowy klucz prywatny do uwierzytelniania telegramów 03925 i rozwiązywania prywatnych adresów źródłowych. Fabrycznie programowane jest losową wartością. Można ją zmienić przez Security Key Write zgodnie z 6.6.4.

6.7.2 Ustawienia domyślne

Pole Default Settings zawiera kopię fabrycznych ustawień: Static Source Address, Security Key, Manufacturer ID i NFC PIN Code. Ustawienia te można przywrócić resetem opisanym w 5.4.

7. Informacje dotyczące zastosowania

7.1 Zasięg transmisji

Na zasięg systemu wpływają przede wszystkim rodzaj i położenie anten odbiornika oraz nadajnika; teren i stopień zasłonięcia drogi radiowej; źródła zakłóceń odbiornika; oraz martwe strefy powstające przez odbicia sygnału od pobliskich obiektów przewodzących.

Ponieważ zasięg silnie zależy od tych warunków, zawsze należy przeprowadzać próby zasięgu, aby ustalić odległość zapewniającą niezawodne działanie w danym miejscu. Poniższe wartości są jedynie orientacyjne:

• Przy bezpośredniej widoczności: zwykle 10 m w korytarzach, do 30 m w halach.

• Przez płyty gipsowo-kartonowe lub suche drewno: zwykle 10 m, przez najwyżej 2 ściany.

• Przez ściany lub stropy żelbetowe: zwykle 5 m, przez najwyżej 1 strop, zależnie od jego grubości.

• Ściany przeciwpożarowe, szyby wind, klatki schodowe i podobne obszary należy traktować jako ekranowane.

Bardzo ważny jest kąt padania sygnału na ścianę. Efektywna grubość ściany, a więc i tłumienie, zależy od tego kąta. Sygnał powinien przechodzić przez ścianę możliwie bezpośrednio. Należy unikać wnęk ściennych.

Zasięg ograniczają także: montaż przycisku na powierzchni metalowej, powodujący do 30% utraty zasięgu; lekkie ściany puste wypełnione wełną izolacyjną na folii metalowej; sufity podwieszane z panelami z metalu lub włókna węglowego; szkło ołowiowe, szkło z powłoką metaliczną oraz meble stalowe.

Odległość między odbiornikiem a innymi urządzeniami emitującymi sygnały wysokiej częstotliwości, np. komputerami oraz sprzętem audio i wideo, powinna wynosić co najmniej 0,5 m. Zakłócenia od innych urządzeń radiowych pasma 2,4 GHz, takich jak routery Wi-Fi, smartfony i bezprzewodowe systemy audio/wideo, mogą mieć duży wpływ na komunikację.

7.2 Konfiguracja odbiornika

03925 przekazuje czynności użytkownika, naciśnięcie lub zwolnienie klawisza, sekwencją telegramów rozgłoszeniowych opisaną w rozdziale 3. Aby zwiększyć prawdopodobieństwo ich odebrania, odbiornik powinien stale nasłuchiwać na wybranych kanałach. Jeżeli to niemożliwe, powinien okresowo nasłuchiwać na jednym z wybranych kanałów przez określony minimalny czas.

Dwa kluczowe parametry odbioru okresowego to odstęp skanowania (scan interval), czyli czas między początkami kolejnych cykli, oraz czas trwania skanowania (scan duration), czyli czas aktywnego nasłuchu w każdym cyklu.

Urządzenie wysyła zdarzenia rozgłoszeniowe z przerwą 20 ms między transmisjami. Wysłanie zdarzenia zajmuje około 1 ms na kanał, czyli około 3 ms dla trzech kanałów. Łączny czas między początkami dwóch zdarzeń wynosi zatem około 23 ms.

Ponieważ odbiornik może rozpocząć skanowanie tuż po początku transmisji, powinien pozostać aktywny przez co najmniej 23 ms, aby sprawdzić początek następnej transmisji. Musi też ponownie uaktywnić się najpóźniej tuż przed początkiem trzeciego zdarzenia. Najdłuższy okres nieaktywności wyznacza zatem czas od początku pierwszego do początku trzeciego zdarzenia, czyli około 46 ms.

Prawdopodobieństwo prawidłowego odbioru zwiększa się po odebraniu więcej niż jednego nadmiarowego zdarzenia. Trzeba też uwzględnić skanowanie różnych kanałów. Z tego powodu teoretyczne maksimum 46 ms powinno być wyraźnie zmniejszone, aby poprawić niezawodność.

Ostatnie zdanie źródła zaleca, gdy stały odbiór jest niemożliwy, „30 ms scan period and 23 ms scan interval”, czyli okres skanowania 30 ms oraz odstęp skanowania 23 ms.

Uwaga do źródła: końcowe nazwy parametrów nie są spójne z wcześniejszym rozróżnieniem odstępu i czasu aktywnego nasłuchu. Przekład zachowuje obie podane wartości i nazwy zamiast samodzielnie zamieniać parametry. Przy implementacji odbiornika należy zweryfikować to zalecenie u producenta.

8. Zasady instalacji

Instalację powinien wykonywać wykwalifikowany personel zgodnie z obowiązującymi w kraju montażu przepisami dotyczącymi instalacji urządzeń elektrycznych.

9. Zgodność z normami

Dyrektywa RED. Normy: EN 60950-1, EN 301 489-17, EN 300 328, EN 62479.

Vimar S.p.A. oświadcza, że urządzenie radiowe jest zgodne z dyrektywą 2014/53/UE. Pełny tekst deklaracji zgodności UE znajduje się w karcie produktu dostępnej na www.vimar.com.

WEEE - informacja dla użytkowników

Symbol przekreślonego pojemnika na urządzeniu lub opakowaniu oznacza, że po zakończeniu użytkowania produktu nie wolno wyrzucać razem z innymi odpadami. Zużyty produkt należy oddać do punktu selektywnej zbiórki albo sprzedawcy przy zakupie nowego urządzenia.

Produkty o wymiarach poniżej 25 cm można oddać bezpłatnie, bez obowiązku zakupu nowego produktu, u sprzedawców o powierzchni sprzedaży co najmniej 400 m². Sprawna selektywna zbiórka do przyjaznego środowisku unieszkodliwienia lub późniejszego recyklingu pomaga ograniczać negatywny wpływ na środowisko i zdrowie ludzi oraz wspiera ponowne wykorzystanie i recykling materiałów konstrukcyjnych.

Dane wydawcy oryginału

03925IEN 01 1806. Vimar S.p.A., Viale Vicenza 14, 36063 Marostica VI, Włochy. www.vimar.com. Strony 2 i 25 oryginału są stronami bez treści instruktażowej. Pełny oryginał, łącznie z okładkami i wszystkimi rysunkami 1-25, znajduje się w dalszej części pliku.

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 **4**
1.1 Basic functionality 4
1.2 Technical data 4
1.3 Environmental conditions 4

2. Functional information **5**
2.1 03925 Device Overview 5
2.2 Basic Functionality 5
2.3 User Interface 5

3. Telegram transmission **6**
3.1 Radio channel parameters 6
3.2 Default radio transmission sequence 6
3.3 User-defined radio transmission sequences 6

4. Telegram format **8**
4.1 Preamble 8
4.2 Access Address 8
4.3 Header 8
4.4 Source address 8
4.5 Check Sum 9
4.6 Payload 10
4.7 Switch status encoding 10
4.8 03925 telegram authentication 10

5. Commissioning **12**
5.1 NFC-based commissioning 12
5.2 Camera-based commissioning 12
5.3 Radio-based commissioning 12
5.4 Factory Reset 14

6. NFC interface **15**
6.1 Using the NFC interface 15
6.2 NFC interface functions 15
6.3 Configuration memory organization 17
6.4 Memory Address Map 18
6.5 Public data 18
6.6 Protected Data 19
6.7 Private Data 22

7. Application information **23**
7.1 Transmission range 23
7.2 Receiver configuration 23

8. Installation rules **24**

9. Standard compliance **24**

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.

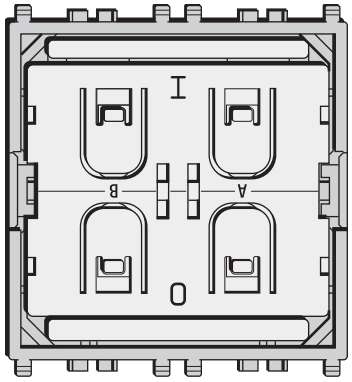


Fig. 1: 03925

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.

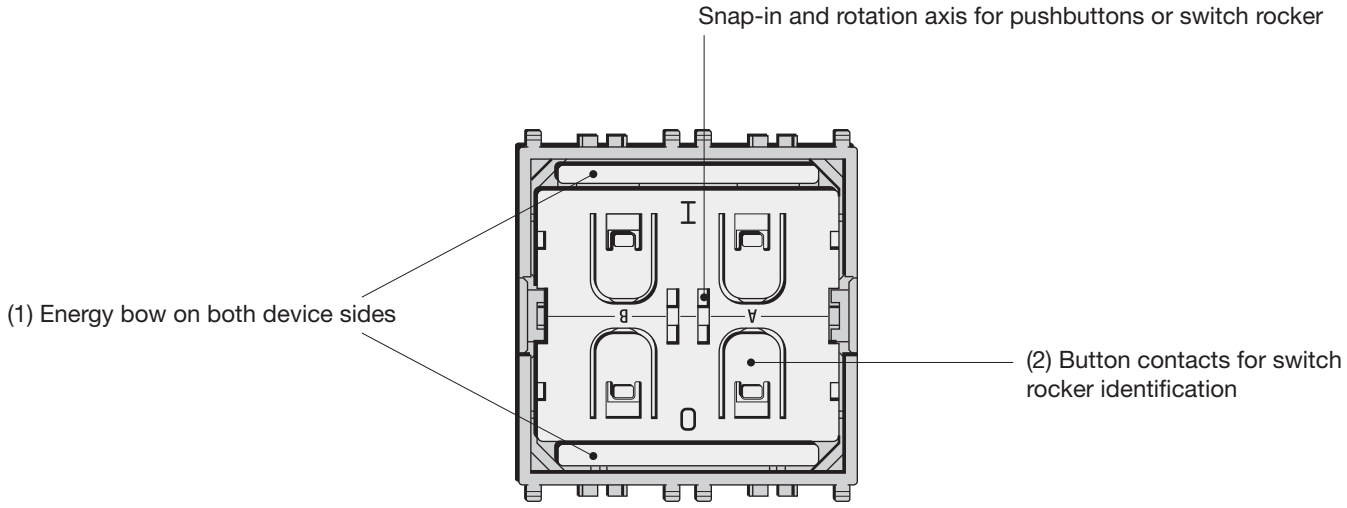


Fig. 2: Electro-dynamic powered pushbutton transmitter module 03925

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:

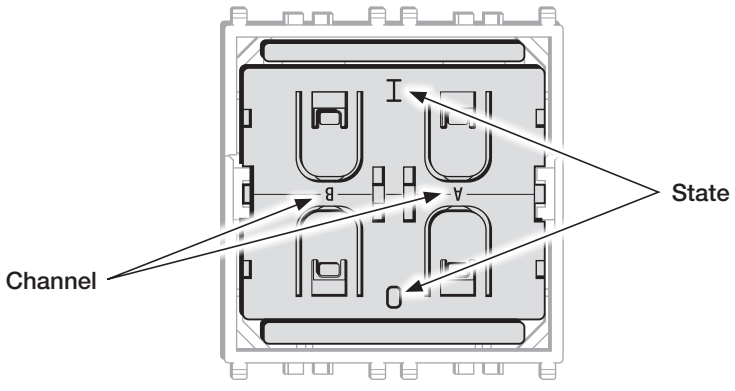


Fig. 3: Button contact designation

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.

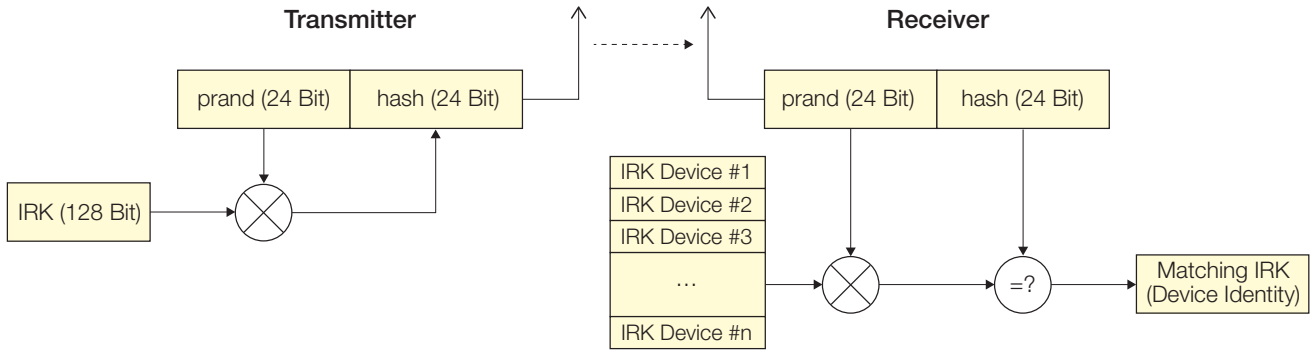


Figure 12 – Resolving private source addresses

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.

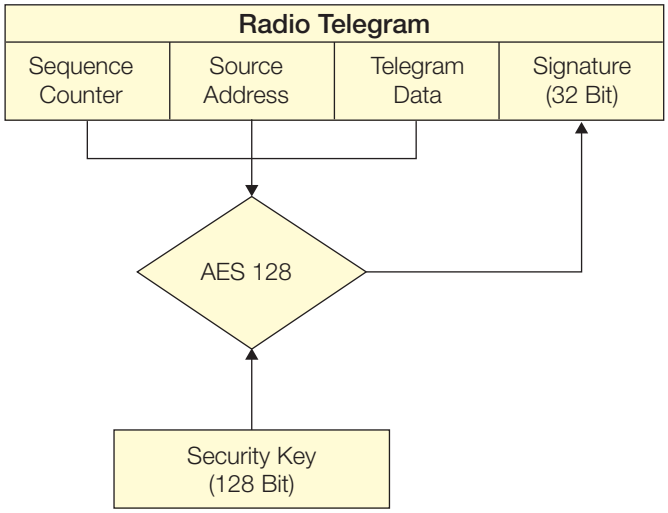


Figure 15 – Telegram authentication flow

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.

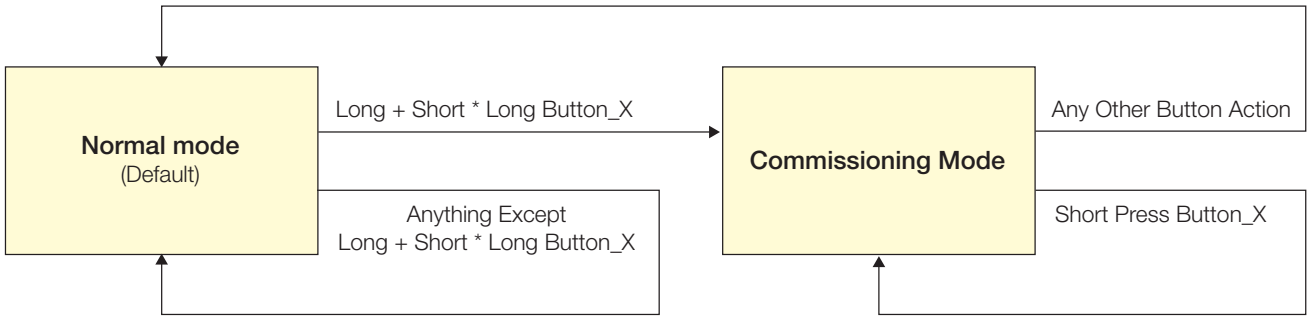


Figure 18 – Button sequence to enter radio-based commissioning mode

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.

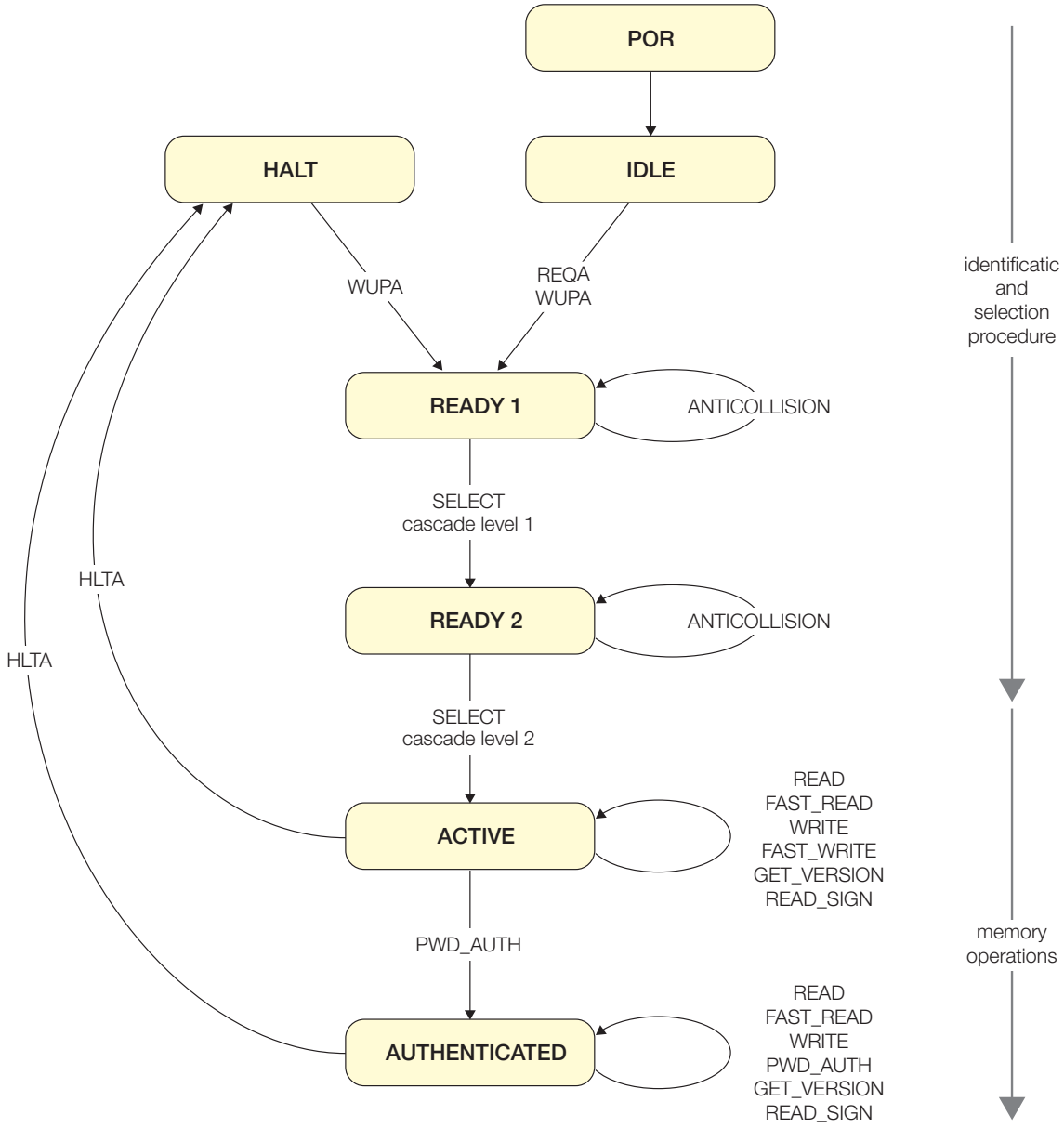


Figure 20 – NFC interface state machine

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.

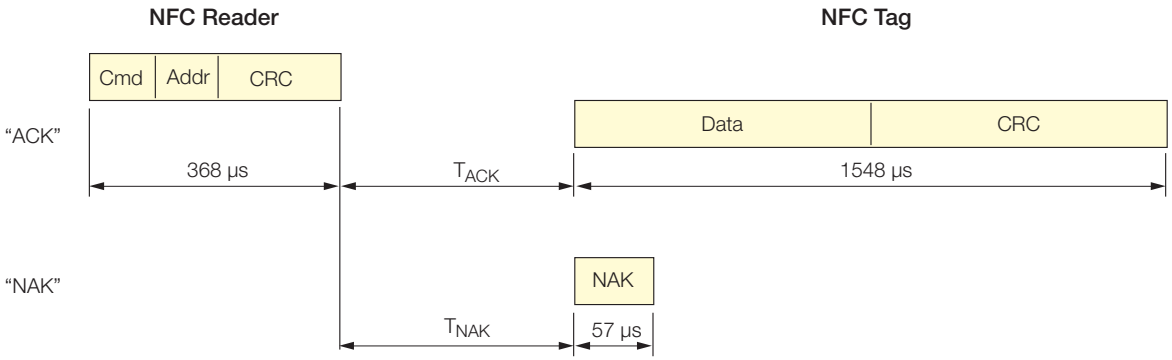


Figure 21 – NFC read command sequence

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.

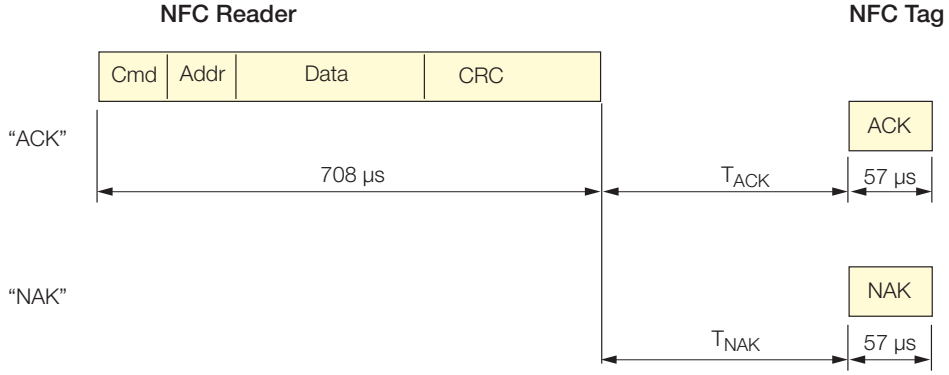


Figure 22 – NFC write command sequence

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.

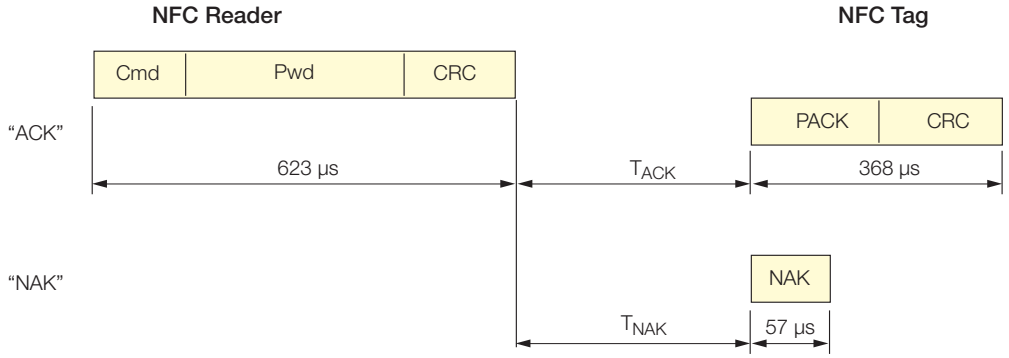


Figure 23 – Password authentication sequence

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