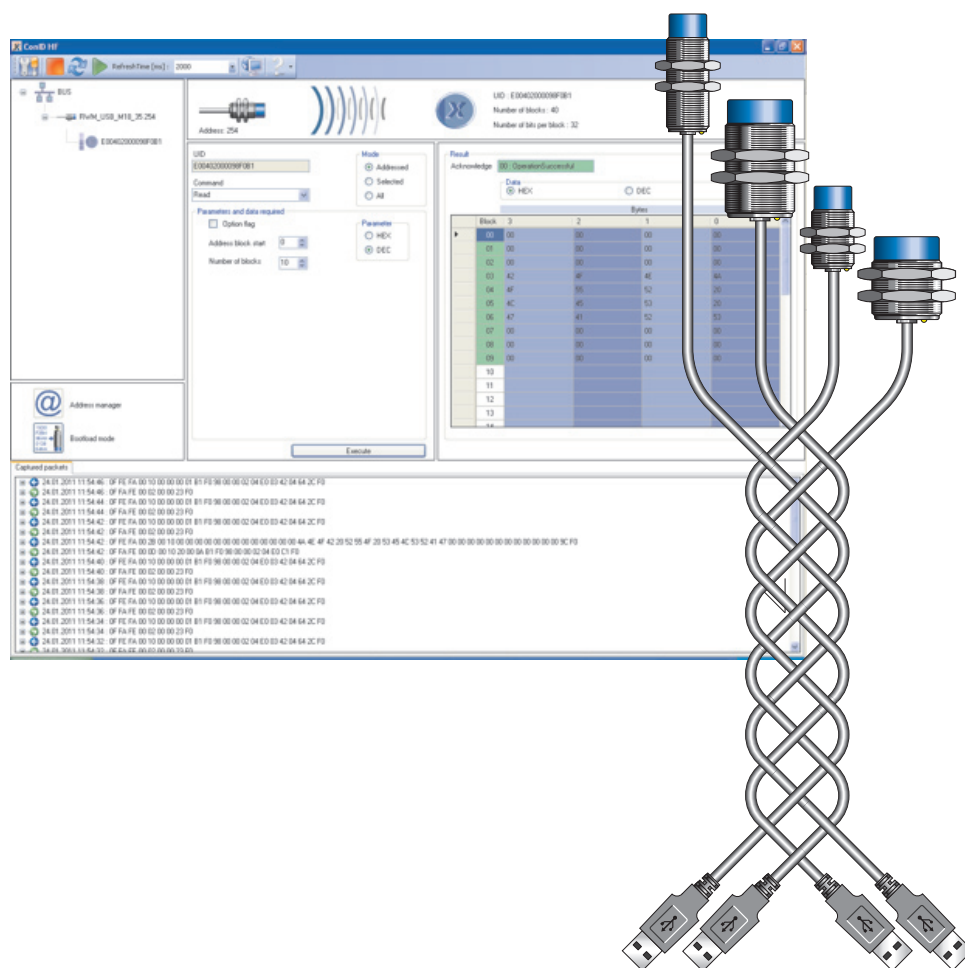


# HANDBOOK

## Read/Write Module HF USB ConID HF Software





# CONTENTS

<b>GENERAL INFORMATION</b> .....	<b>1</b>
USB HF READ /WRITE MODULE .....	1
Configuration of the USB HF Read/Write Module (RWM).....	1
REMINDER: CODING .....	1
<b>REQUIRED SOFTWARES</b> .....	<b>3</b>
<b>INSTALLATION OF THE DRIVERS</b> .....	<b>3</b>
Loading the installation software for the USB RWM driver .....	3
Installation of the USB HF RWM.....	4
Virtual communication port allocated to the USB HF RWM .....	5
Uninstallation of the driver.....	5
Introduction.....	6
Installation of the ConID HF Software.....	6
Uninstallation of the ConID HF Software program .....	8
<b>ConID HF SOFTWARE</b> .....	<b>9</b>
<b>STRUCTURE OF THE PROGRAM</b> .....	<b>9</b>
Bootloader.....	15
<b>COMMANDS CONCERNING THE READ/WRITE MODULE (RWM)</b> .....	<b>16</b>
30h Set Field .....	17
31h Get Field.....	18
32h Write RWM .....	19
33h Read RWM.....	20
34h RWM Info .....	21
35h Sleep Mode .....	22
36h Reset.....	23
3Bh Set Protection Mode .....	24
3Ch Get Protection Mode.....	25
3Fh Read RWM UID .....	26
<b>COMMANDS CONCERNING THE TRANSPONDER (TAG)</b> .....	<b>27</b>
00h Status .....	27
Generalities .....	29
10h Read.....	30
11h Write .....	31
12h Lock (block).....	32
Transponder states.....	33
13h Stay quiet .....	34
14h Select .....	35
15h Reset To Ready.....	36
16h Write AFI.....	37
17h Lock AFI .....	38
18h Write DSFID .....	39
19h Lock DSFID .....	40
1Ah Get Info .....	41
20h Get Random Number .....	42
21h Set Password .....	43
22h Write Password .....	44
23h Lock Password.....	45
24h 64 bit Password Protection.....	46
25h Protect Page.....	47
26h Lock Page Protection Condition .....	48
27h Get Protection Status .....	49
28h Destroy TAG.....	50



# GENERAL INFORMATION

## USB HF READ /WRITE MODULE

### Configuration of the USB HF Read/Write Module (RWM)

#### USB RWM

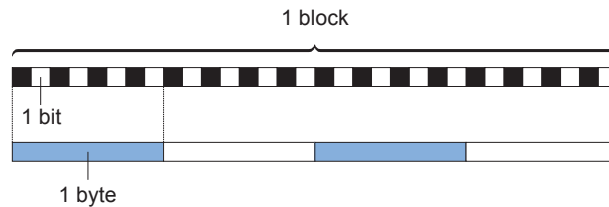
The USB RWM can be connected directly to the USB port of a PC. The power supply of the RWM is provided by the computer's USB port.



## REMINDER: CODING

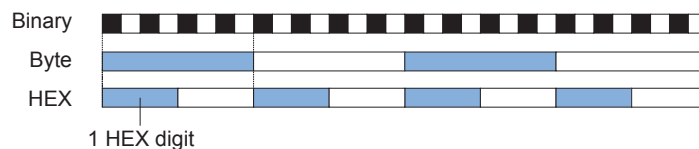
#### Binary code

Each block is composed of 4 byte or 32 bit, a byte being a 8-bit word.



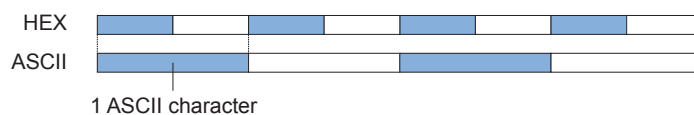
#### Hexadecimal code (HEX)

To simplify writing, it is usual to code the byte in 2 HEX digits, an HEX digit consisting of a group of 4 bits. This hexadecimal coding (HEX) includes the numbers 0 to 9 and the letters A to F (16 different digits which reflect the 16 possible combination of 4 bit).



#### ASCII Code

If text more explicit than HEX needs to be written in the memory, then ASCII code (American Standard Code for Information Interchange), which requires 2 HEX digits for each character, is used.



For information, below are given the ASCII codes, expressed in HEX, as they are used in the ConIdent® read/write module.

It should be noted that

- non-printable characters (LF, FF, etc.) with hexadecimal codes ≤ 1F are represented by “\*”,
- the characters with a hexadecimal code ≥ 7F are represented by “?”.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
1	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
2	SP	!	“	#	\$	%	&	‘	(	)	*	+	,	-	.	/
3	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
6	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7	p	q	r	s	t	u	v	w	x	y	z	{		}	~	?

# REQUIRED SOFTWARES

## INSTALLATION OF THE DRIVERS

### Loading the installation software for the USB RWM driver

#### Start-up

To start the driver installation, double-click the icon corresponding to the installation program.

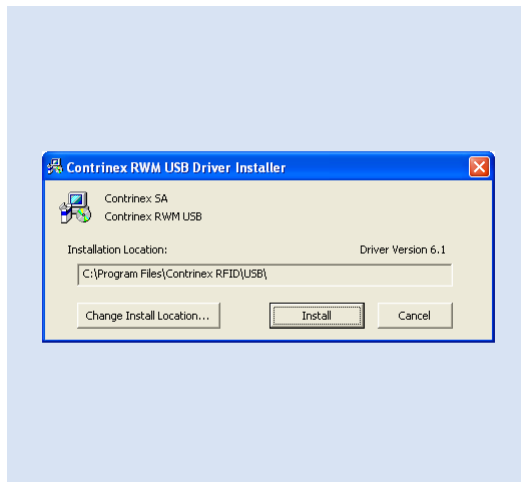


RWM USB Driver.exe

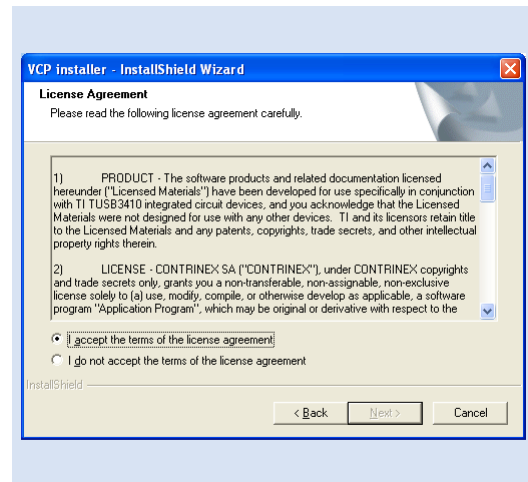
RWM USB Driver is compatible with Windows 2000 and Windows XP

#### Installing the installer

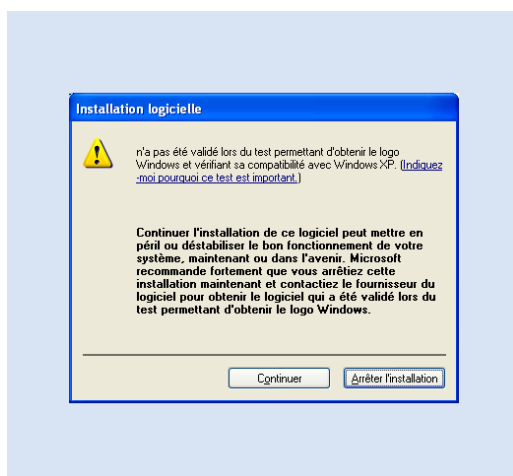
The installer is the software that will allow installation of the drivers. The program starts and the following displays appear in succession:



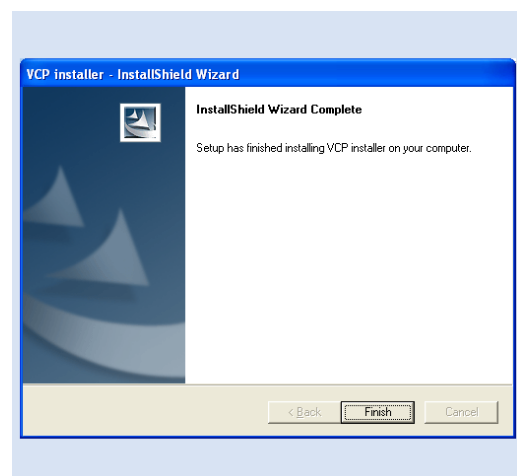
1. Installer configuration



2. License agreement.  
Check "I accept the terms of the license agreement".



3. Warning  
Each time this warning appears, click on "Continue".



4. Installation of the installer completed.  
Click on "Finish".

# Installation of the USB HF RWM

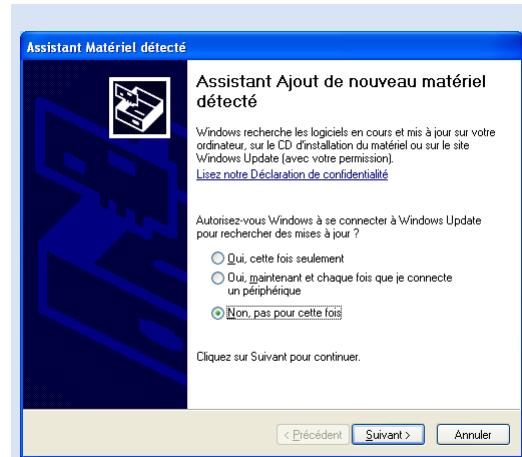
## USB Connection

Establish the USB connection between the control console (PC) and one of the USB HF RWM (RLS-1181-120, RLS-1181-220, RLS-1301-120 or RLS-1301-220).

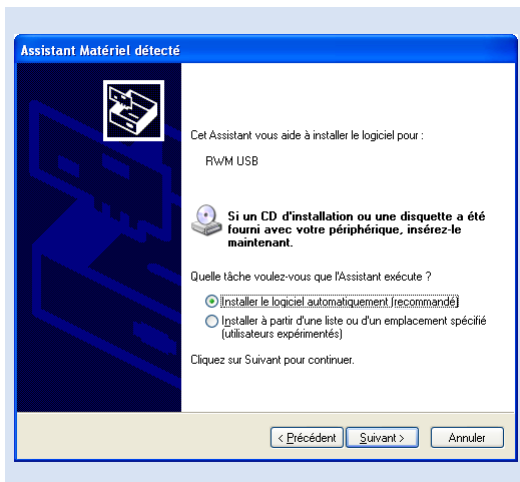
## Installing the material



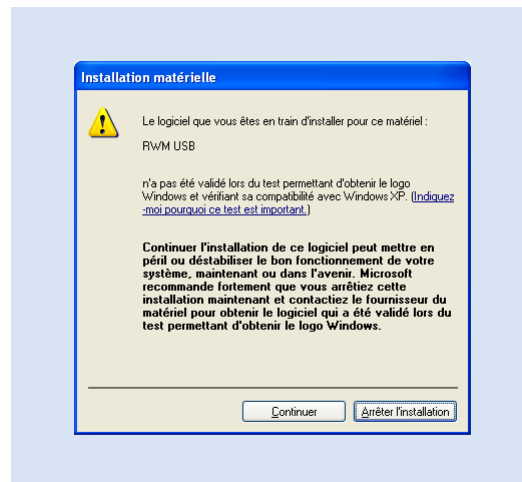
1. The RFID HF Starter kit is detected as soon as the USB connection is established.



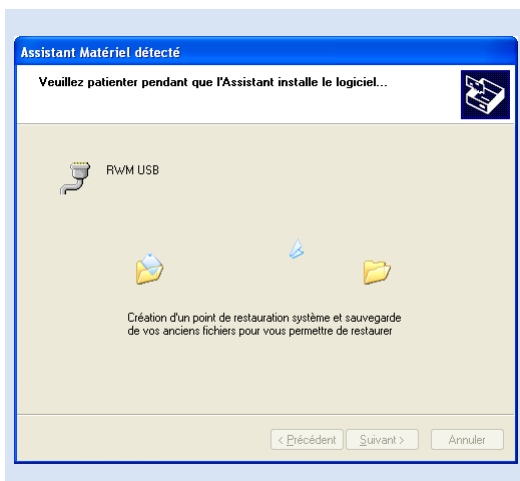
2. Decline the invitation to look for updates.



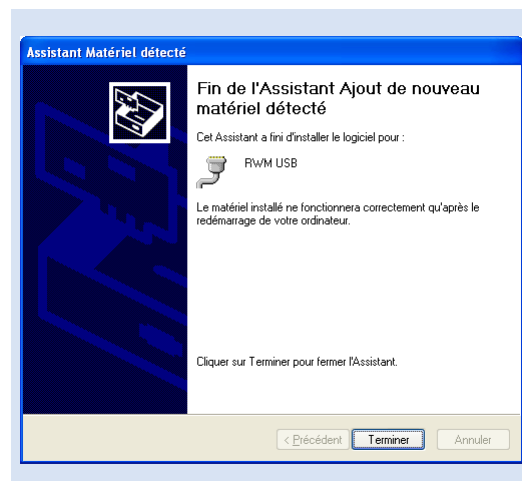
3. Install the software automatically.



4. The software does not need to be validated. Click on “**Continue**”.



5. Installation of the software for the material.



6. The software specific to the RFID Adaptor has been installed. Click on “**Finish**”.





7. The new material is ready for use.

## Virtual communication port allocated to the USB HF RWM

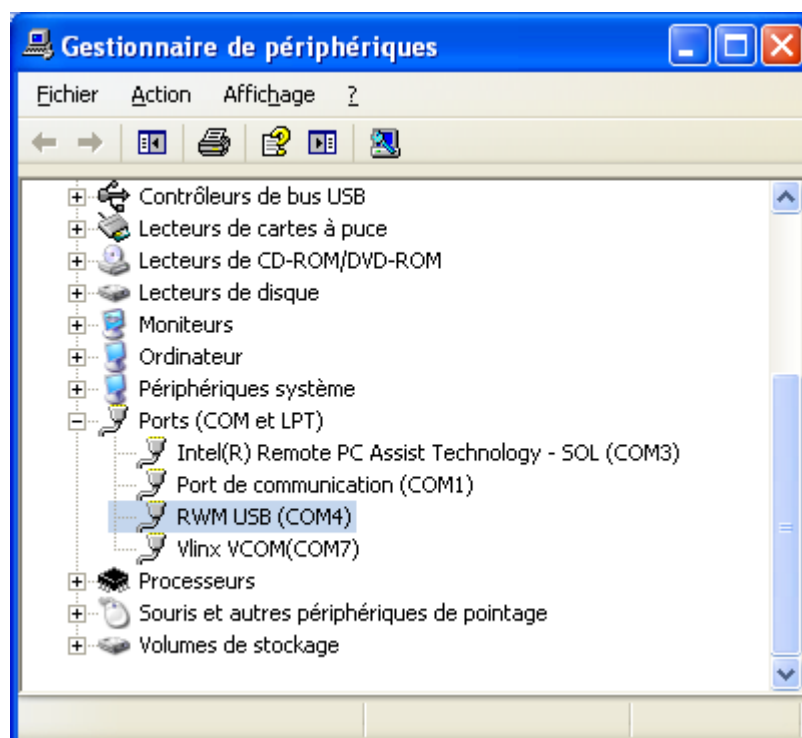
### Introduction

When using the USB HF RWM, especially in conjunction with **ConID HF Software**, the identity of the virtual communication port assigned to the material must be known.

### Utilization with the USB HF RWM

The COM port assigned can be found by consulting the Peripheral manager (Start - Parameters – Configuration menu – System – Material - Peripheral manager).

The virtual COM port allocation can be found in the **Ports (COM and LPT)** file.



## Uninstallation of the driver

### Uninstallation

To remove the driver, go to Add/Remove Programs in the Control Panel.

# INSTALLATION OF ConID HF SOFTWARE

## Introduction

### Objectives

The **ConID HF Software** program is designed to familiarize users didactically with ConIdent® HF systems (CONTRINEX RFID).

With the RFID HF Starter kit, the user may work directly from a PC with several (up to 10) Read/Write Modules (RWM) connected to a RS485 fieldbus. The user can familiarize himself with the commands related to these modules, as well as to the transactions that can be programmed in order to read, to modify or to protect the contents of transponder memory.

ConID Software is compatible with Windows XP, Windows Vista and Windows 7.

### Note

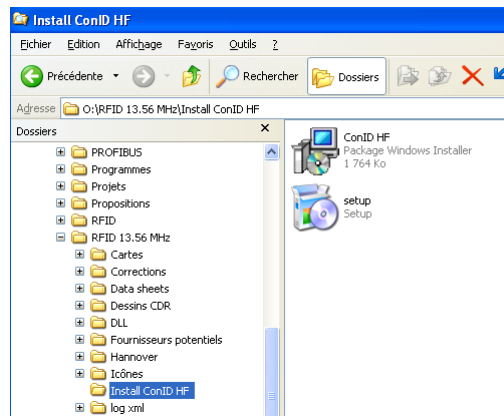
The commands specific to RWMs and to transactions between RWMs and transponders are detailed in the RWM specifications (data sheets).

A detailed description of CONTRINEX transponders memory can be found in the data sheets of the transponders. For a use with other transponders, compatible with ISO 15693 standard, please refer to the specifications of the manufacturer.

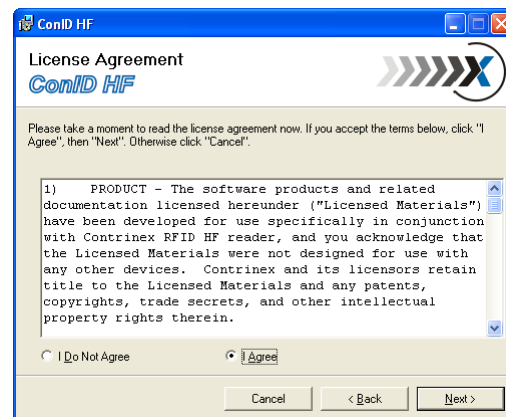
## Installation of the ConID HF Software

### Installation start-up

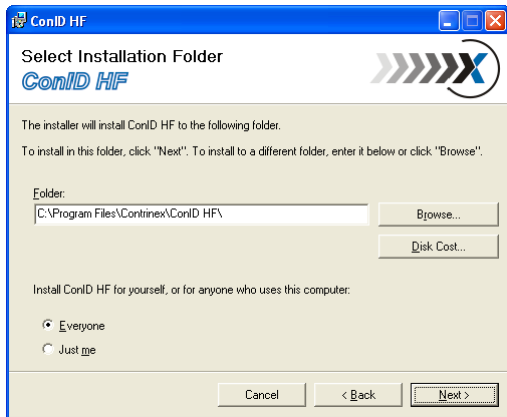
To start installation of the ConID Software program, double-click on the icon “**Setup**”.



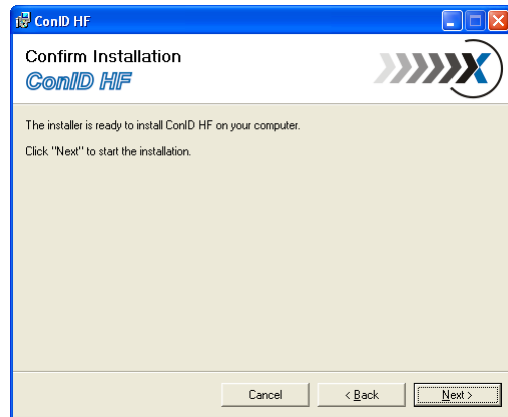
1. Welcome window indicates that ConID HF program is about to be installed on your computer. Click on “**Next**”.



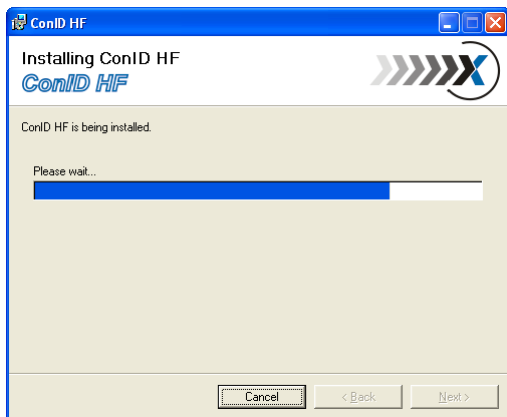
2. After having read and approved the license agreement, click on “**Next**”.



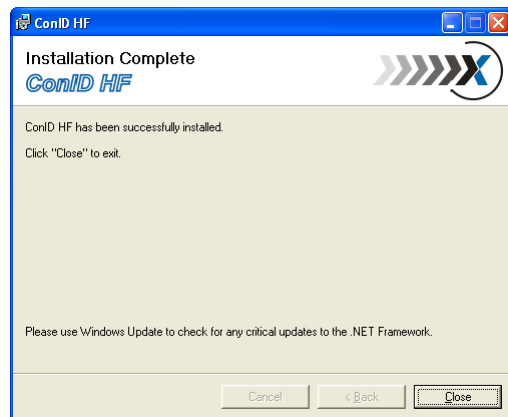
3. Choose the folder where the program has to be installed. Click on **“Next”**.



4. If you agree with everything, click on **“Next”** to start the installation.

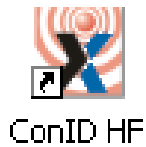


5. The program is being installed.



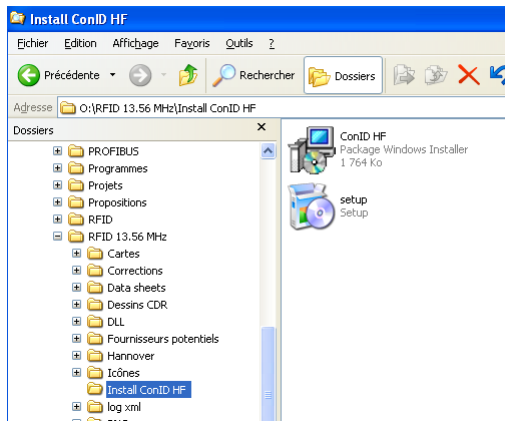
6. The program has been successfully installed. You can exit the installation by clicking on **“Close”**

The icon ConID HF was also placed on the desk top.

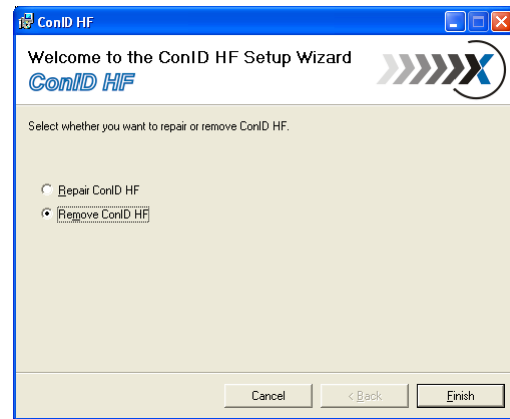


# Uninstallation of the ConID HF Software program

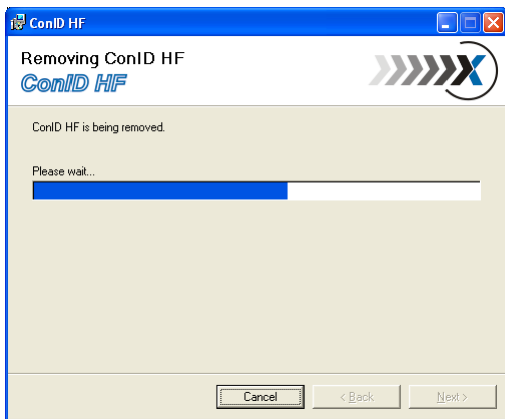
How to proceed?



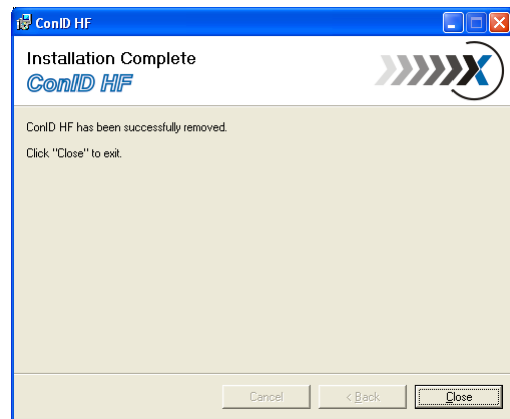
1. To start uninstallation or repair of the ConID Software program, double-click on the icon "Setup".



2. The program proposes to repair the software or to remove it. Repairing is, in fact, a new installation.



3. Uninstallation is in progress.



4. ConID HF software has been removed. Click on "Close" to exit.

# ConID HF SOFTWARE

## STRUCTURE OF THE PROGRAM

### Launching the program

When ConID HF Software is launched, the following screen will be displayed where different options must be entered:

Initialization

Baudrate: 115200

Com port number: 3

Master adresse: 250

Address scan zone: Start 0, Stop 9

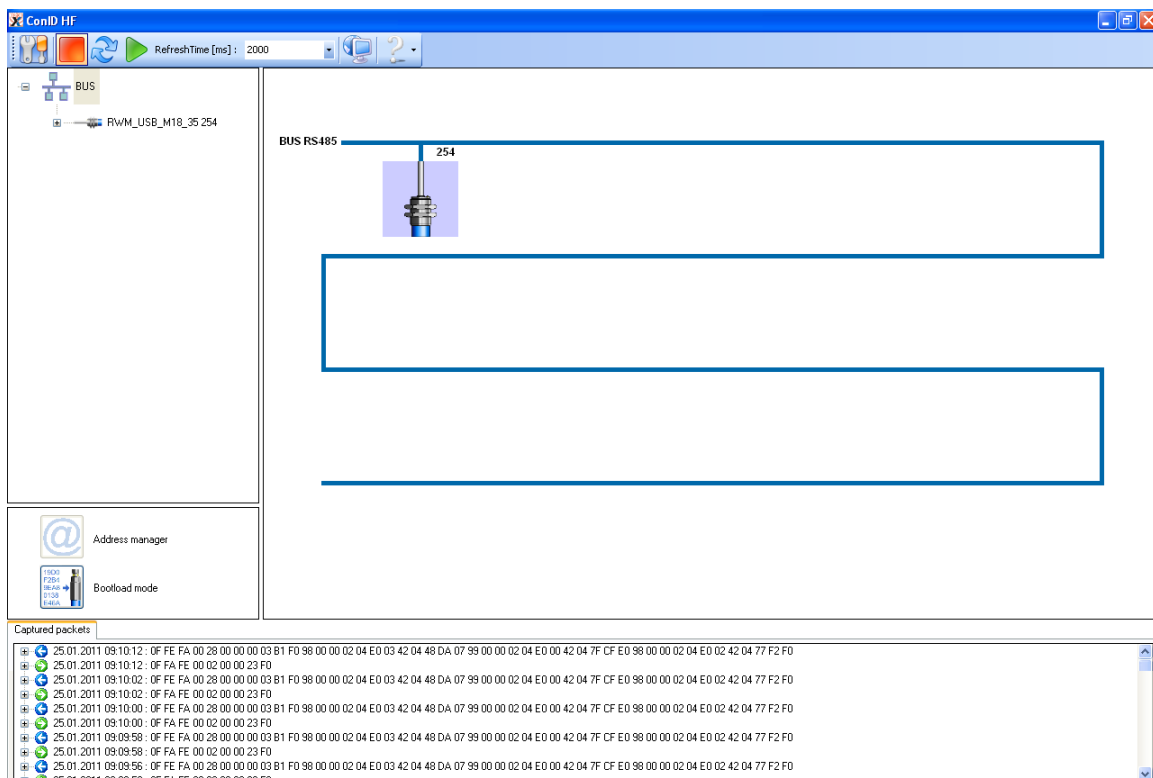
Set configuration

Memorize parameters to apply them automatically on next start

Reading network structure

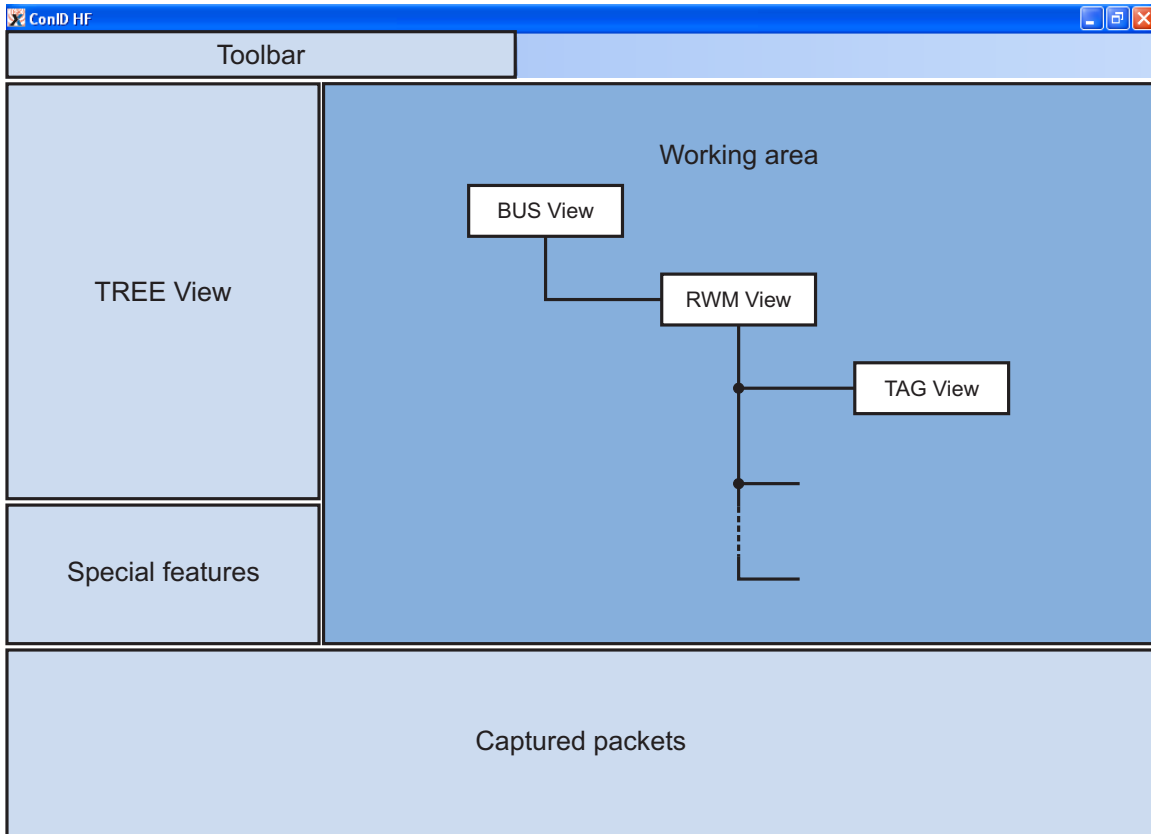
- Data transfer rate (Baudrate)
- Virtual COM port number allocated during installation of the drivers
- Master address is defined during the initialization
- The logical address of the USB HF RWM is always 254. Also the “Address scan zone” can be as short as possible: from 254 to 254:

When these options are introduced, click on “Set configuration” and the very short configuration process takes place and result in the window below.

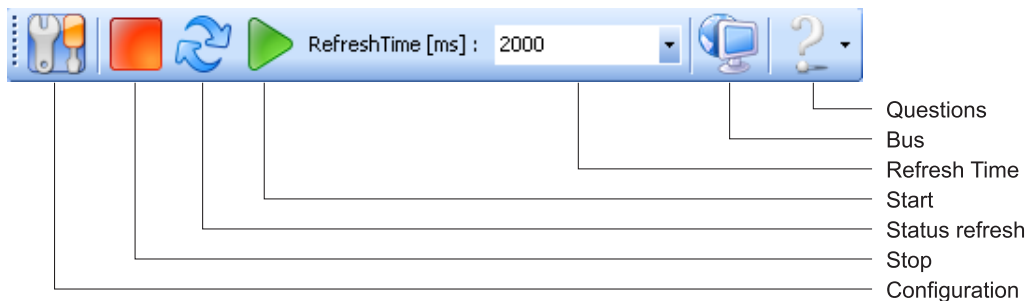


## Structure of the various displays

The displays are all configured on the same schema illustrated below. The light blue parts are always present.



## Toolbar



The **Configuration** button allows to redo a configuration in order to determine the RWMs which are plugged on the bus. Normally, the RWM plugged on the bus are periodically scanned to determine which transponders are in front of them. It is possible to stop the scanning process by pressing the **Stop** button.

Pressing the **Status refresh** button initiate one scanning cycle.

The **Start** button restart the scanning process when it has been stopped.

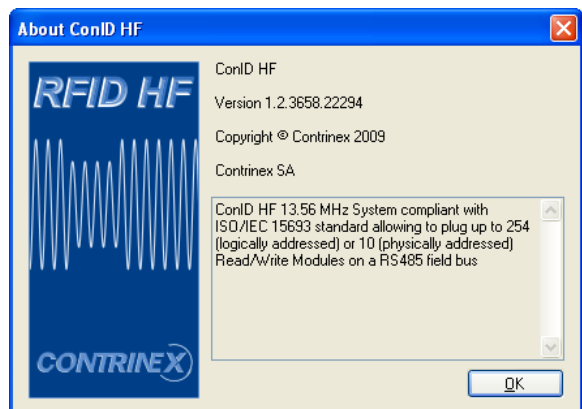
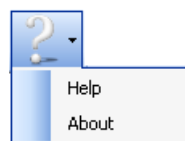
It is possible to fix the **Refresh time**, that means the period between scanning.

The **Bus** button switches to the Bus view screen.

Pressing the **Questions** button opens the following menu:

The **Help** item returns to the data sheets, always updated, on the Contrinex Web site.

The **About** item opens the following display:



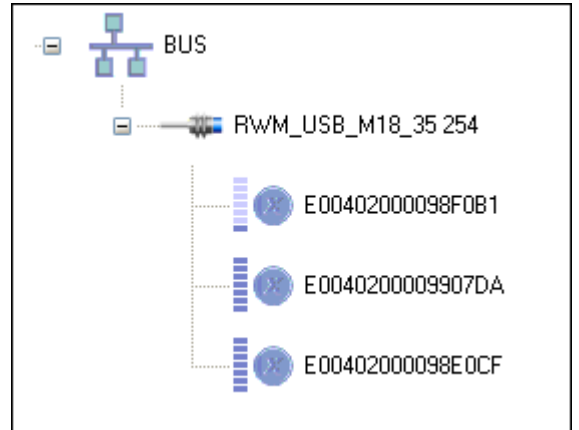
### Tree view

The Tree view is an important feature because it gives the complete structure of the field bus.

The USB HF RWM is represented with its type and is identified by its address (254).

When expanded, the transponders in front of the corresponding RWM are represented. They are identified by their unique identification number (UID).

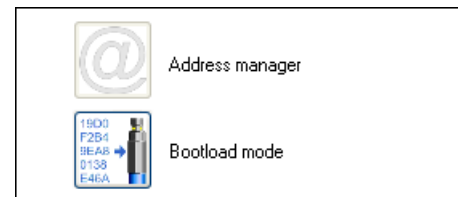
The height of the bar beside the transponder indicates the quality of the received signal by the RWM.



### Special features

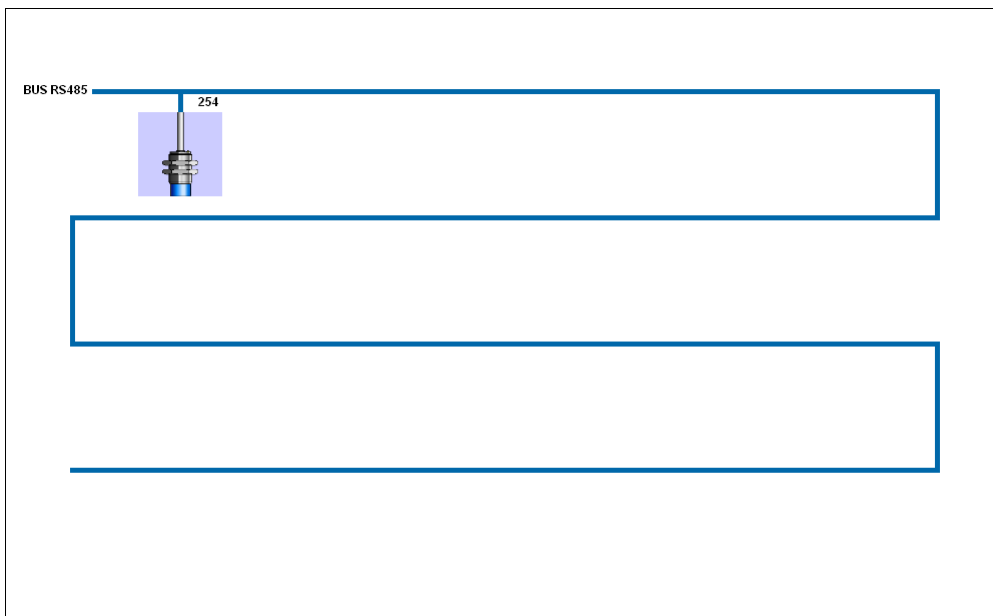
There are two features which are accessible with this display:

- when used with an USB adaptor, the Address manager allows to choose the type of address of the RWM (physical or logical) and to assign, if necessary, a logical address. This feature is inoperative when ConID Software is used with an USB HF RWM because its logical address is fixed to 254 and cannot be changed.
- the **Bootload mode** which allows to update the firmware of the RWM.



### BUS view

In this case, the Bus view is not very interesting. Nevertheless, it shows the RS485 field bus and the USB HF RWM connected to it and identified by its type and its fixed address (254).



### RWM view

The RWM view is divided into two parts. The first part relates to the RWM directly and the second one gives a list with some details of the transponders which are in front of the RWM.

The part related to the RWM has always the same structure:

- the type of RWM, its address and the version of the firmware
- a scroll list where the command has to be chosen,
- data required to execute the command (if necessary, depending on the command),
- “Execute” button,
- Result of the command with an acknowledge which gives information on the course of the command and data if necessary (depending on the command).

### TAG view

The TAG view is divided into three parts. The upper part shows which transponder in front of which reader is concerned. The left lower part is dedicated to the command and the right lower part is dedicated to the result of this command.



A command placed in **Addressed mode** relates to the transponder whose address is specified.

Address: 254

UID : E0040200009907DA  
Number of blocks : 40  
Number of bits per blocks : 32

UID: E0040200009907DA

Command: [dropdown]

Mode:  Addressed,  Selected,  All

Result: Acknowledge [input]

A command placed in **Selected mode** relates to a transponder which has been selected before.

Address: 254

UID: E0040200009907DA

Command: [dropdown]

Mode:  Addressed,  Selected,  All

Result: Acknowledge [input]

Certain commands can be placed in **All mode**, that means that all the transponder in front of the RWM are concerned.

Address: 254

UID: [input]

Command: [dropdown]

Mode:  Addressed,  Selected,  All

Result: Acknowledge [input]

In addition, the left lower part contains a scroll list where the command has to be chosen and a group where parameters and data required are to be entered. In this group, it is always possible to activate the option flag which can be optional or necessary for certain commands and/or certain manufacturers.

Parameters introduced can always be expressed in HEX or DEC format. The selected format applied also for the numbering of the blocks in the result display.

Data can be expressed in HEX, DEC or ASCII format. This is valid as well in the commands as in the results.

When parameters and data are correct, the **“Execute”** button has to be clicked in order to perform the operation.

In the result group, the acknowledge which gives information on the course of the command is always present. In addition, data returned by the transponder (depending on the command) are displayed.

### Captured packets

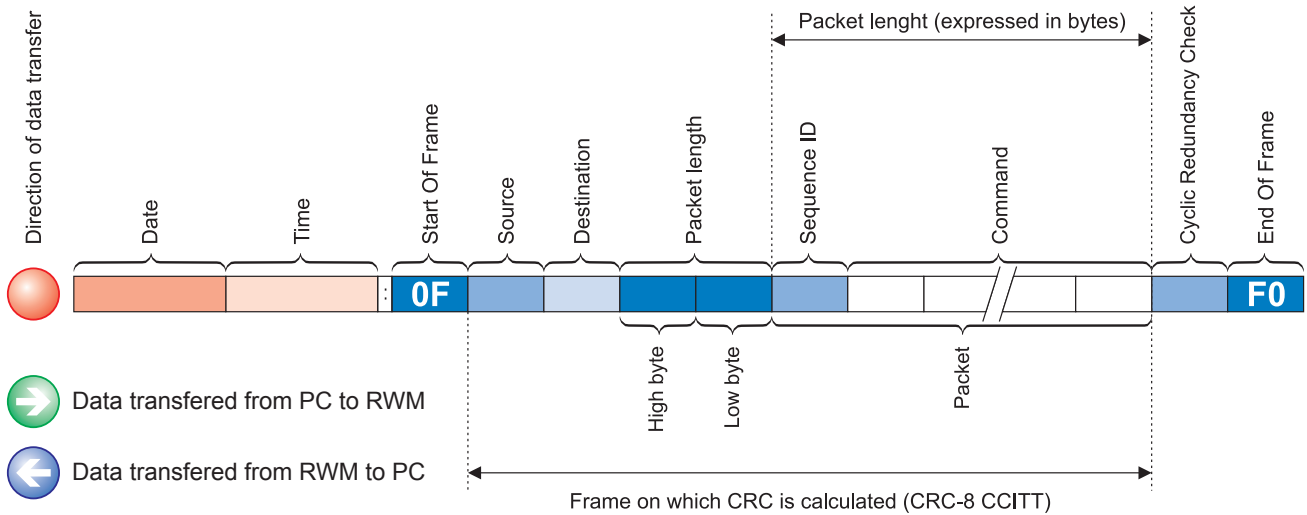
This display shows chronologically the transactions which occur between the RWM and the transponder. Each transaction can be expanded in order to see it in a more explicit representation.

A maximum of 100 transactions (100 captured packets) can be stored.

Captured packets	
	25.01.2011 11:33:45 : 0F FE FA 00 28 00 00 03 B1 F0 98 00 00 02 04 E0 03 42 04 48 DA 07 99 00 00 02 04 E0 00 42 04 77 CF E0 98 00 00 02 04 E0 02 42 04 77 AB F0
	25.01.2011 11:33:45 : 0F FE FA 00 02 00 00 23 F0
	25.01.2011 11:20:58 : 0F FE FA 00 11 00 1A 00 0F DA 07 99 00 00 02 04 E0 00 00 28 04 02 F1 F0
	25.01.2011 11:20:58 : 0F FE FA 00 03 00 1A 10 9D F0
	25.01.2011 10:56:17 : 0F FE FA 00 11 00 1A 00 0F DA 07 99 00 00 02 04 E0 00 00 28 04 02 F1 F0
	25.01.2011 10:56:17 : 0F FE FA 00 03 00 1A 10 9D F0
	25.01.2011 10:56:14 : 0F FE FA 00 03 00 14 00 76 F0
	25.01.2011 10:56:14 : 0F FE FA 00 0B 00 14 20 DA 07 99 00 00 02 04 E0 A7 F0

Time ↑

The structure of the captured packets is represented below.



**Possible options on the captured packets**

While clicking on the right button of the mouse, a list of possible options will be revealed.

It is thus possible to expand each packet in order to become an explanation on the different bytes exchanged. When expanded, it is also possible to collapse the packet to obtain its condensed form.

It is possible to export the list in a log file or to import such a list in order to examine it.

Each packet can be printed.

Each packet can be cleared.

- Expand all
- Expand
- Collapse all
- Collapse
- Export
- Import
- Print all
- Print selected packet
- Clear all
- Clear selected packet

# Bootloader

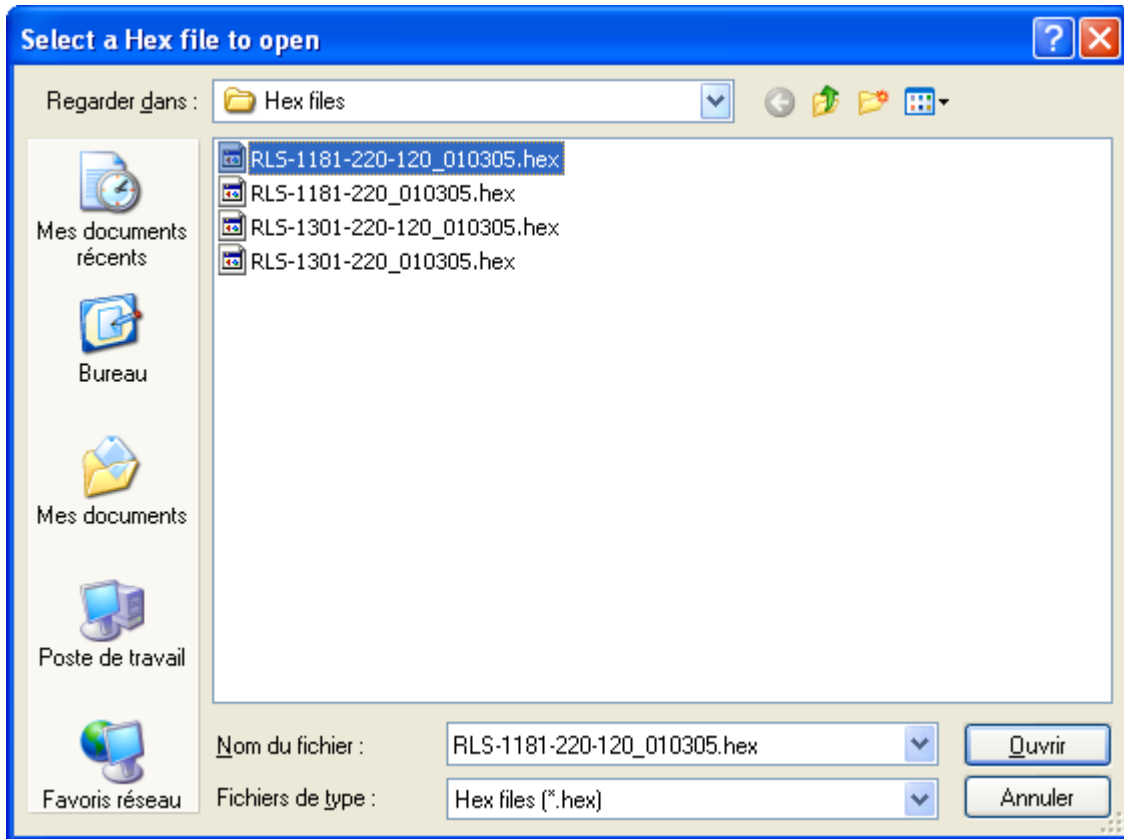
## Introduction

The Bootloader allows to update the firmware of the RWM.

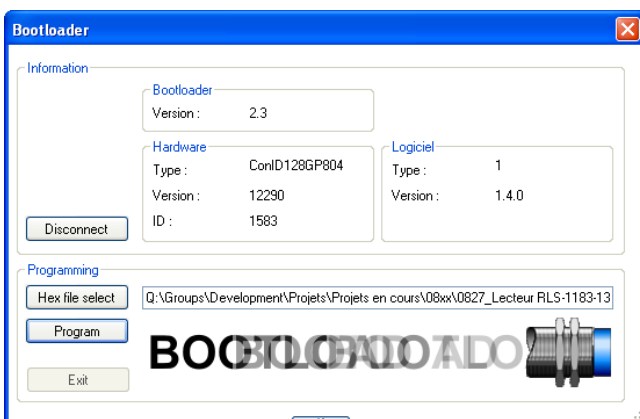
When an upgrade of the firmware of the RWM will be done, a new .hex file will be put on Contrinex Website and the user can load this firmware in its RWM by the mean of the Bootloader.

## Loading the firmware

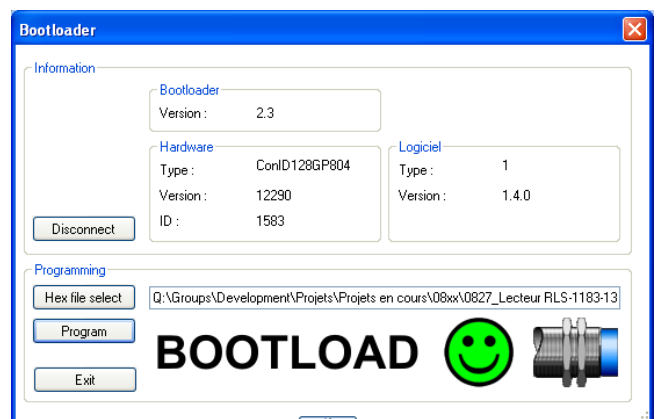
The correct .hex file must be selected.



When it is done, the upgrade starts by clicking on "Program".



During bootload...



Bootload completed with success.

When the operation is finished, do not forget to make a new configuration.

## COMMANDS CONCERNING THE READ/WRITE MODULE (RWM)

### Introduction

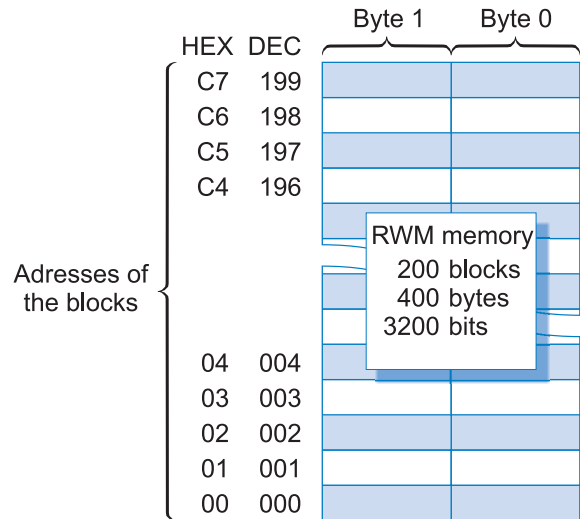
In the RFID HF system, there are commands dedicated specifically to the Read/Write Module. It is thus possible to manage the electromagnetic field of the RWM, to write or read information in the memory of the RWM.

When one works with protection, the RWM must always be active. It is for that reason that we must set the RWM in protection mode.

### Structure of the memory of RWM

The user part of the memory of an RWM has a capacity of 3200 bits and is organized in 200 blocks of 2 bytes each.

In the user memory of the RWM, it is possible to write or to read one block at a time.



### List of the commands

The list of the commands dedicated to the RWM is accessible in the scroll list "Command". The various commands with their meaning are listed below.

#	Name	Meaning
30h	Set Field	Controls the magnetic field
31h	Get Field	Informs on the state of the magnetic field
32h	Write RWM	Stores the value of the two bytes entered at the specified address
33h	Read RWM	Reads the block with the specified address
34h	RWM Info	Returns information on the firmware and the type of RWM
35h	Sleep Mode	Decreases the consumption by approximately 50%.
36h	Reset	Start RWM again
3Bh	Set Protection Mode	Defines the protection mode of the RWM
3Ch	Get Protection mode	Returns the state of the protection mode of the RWM
3Fh	Read RWM UID	Returns the UID of the RWM

### Convention

Decimal numbers will be followed by letter d: ex. 12d.

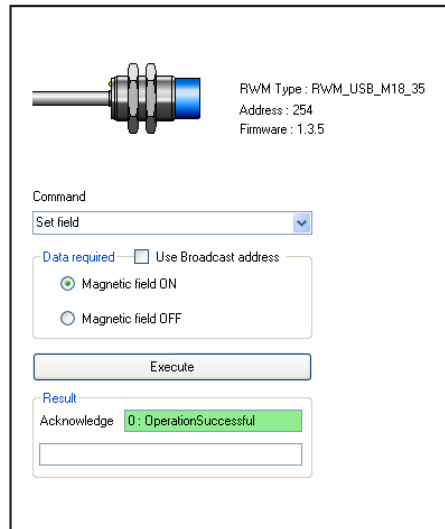
Hexadecimal numbers will be followed by letter h: ex. 1Ah = 26d

Binary numbers will be followed by letter b: ex. 1101b = 13d

## 30h Set Field

### Effect of the command

Controls the magnetic field of the RWM.



### Command

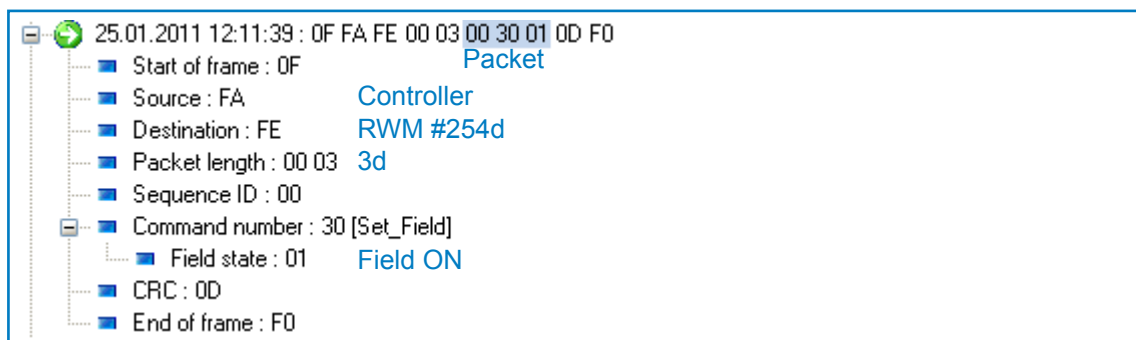
The broadcast address FFh can be used if we want to set the same state of the magnetic field for all the RWMs.

Data required to set the state of the magnetic field:

- Magnetic field ON (01) or OFF (00).

Field OFF decreases the consumption by approximately 40%.

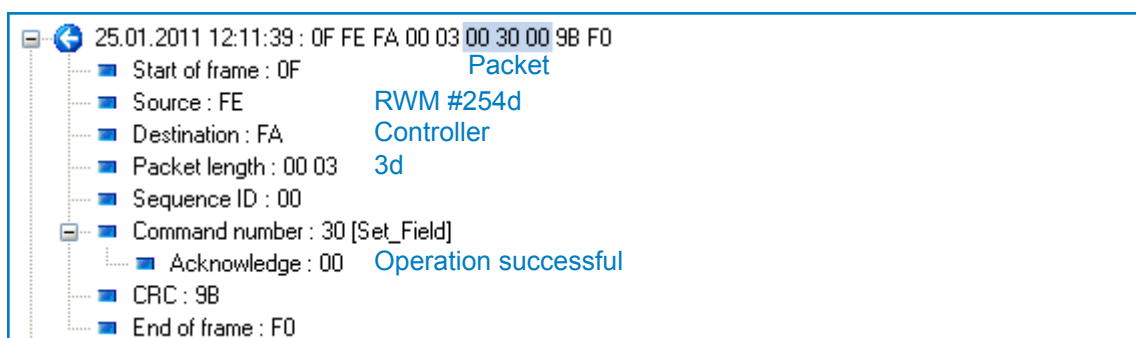
The figure beside shows the detail and the meaning of the bytes sent from the Controller to the RWM.



### Answer

The figure beside shows the detail and the meaning of the bytes sent from the RWM to the Controller.

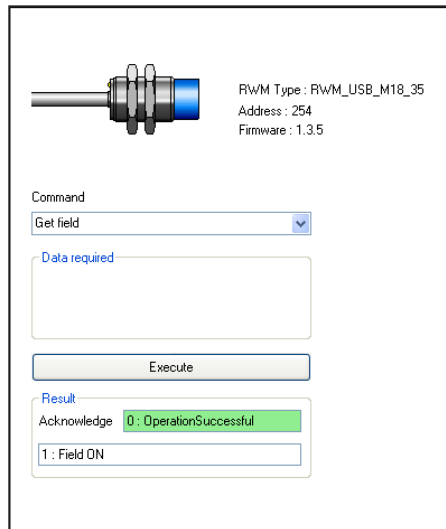
If the broadcast mode has been chosen, there is no answer from the RWMs.



## 31h Get Field

### Effect of the command

Returns information on the state of the magnetic field

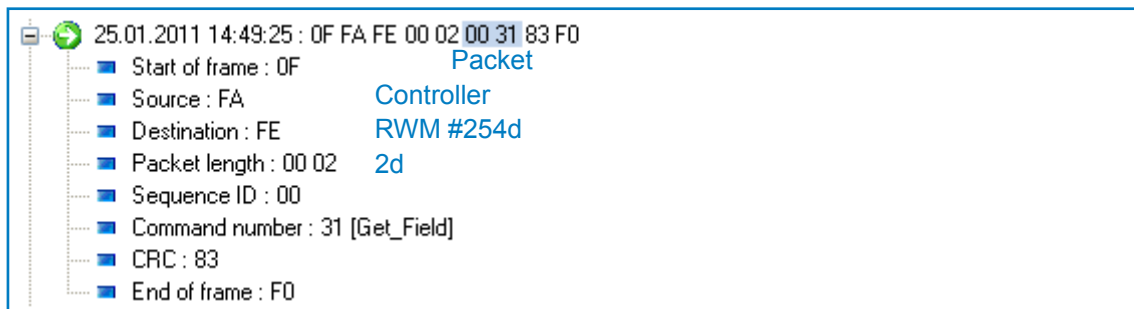


### Command

Data required to get the state of the magnetic field:

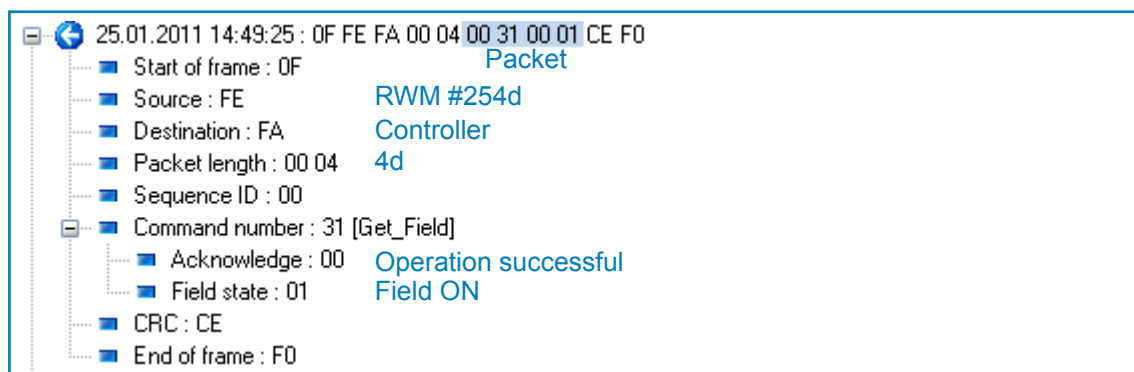
- None.

The figure below shows the detail and the meaning of the bytes sent from the Controller to the RWM.



### Answer

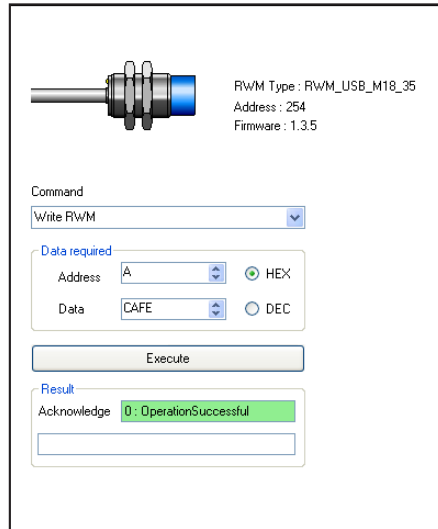
The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.



## 32h Write RWM

### Effect of the command

Stores the value of the two bytes at the specified address

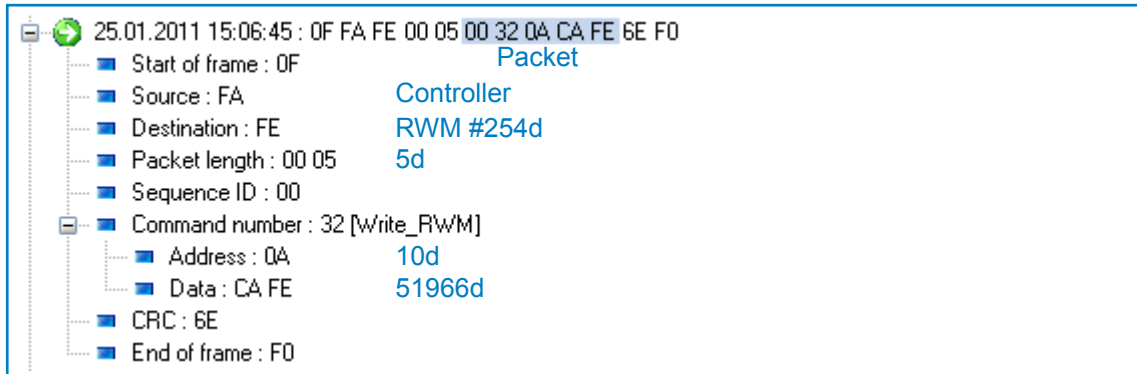


### Command

Data required to write one block in the RWM:

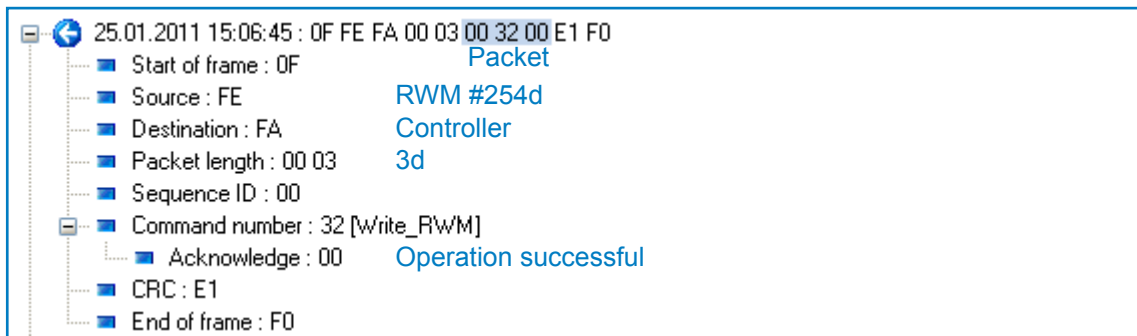
- The address of the block to write
- Data to write

The figure below shows the detail and the meaning of the bytes sent from the Controller to the RWM.



### Answer

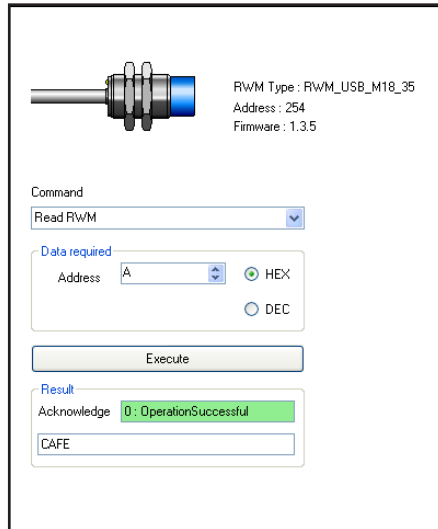
The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.



## 33h Read RWM

### Effect of the command

Reads the block with the specified address

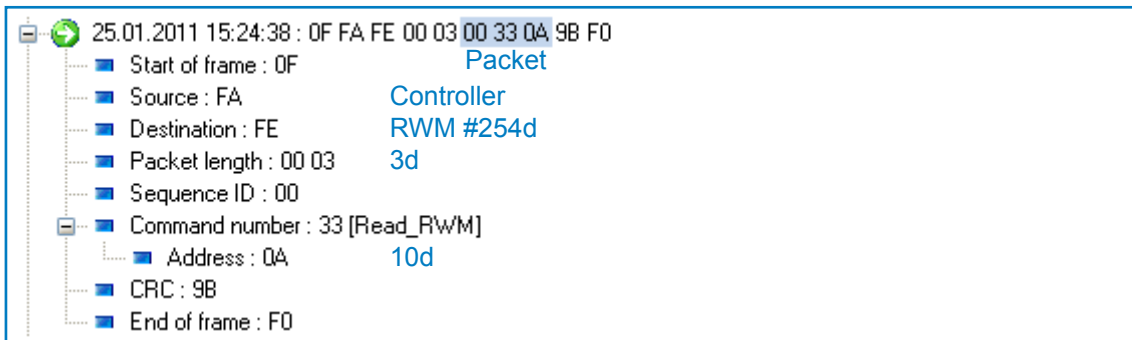


### Command

Data required to read one block in the RWM:

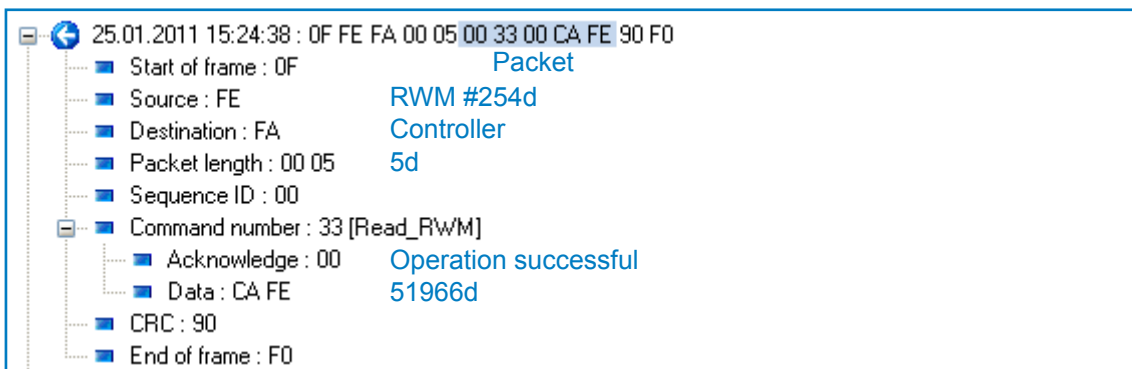
- The address of the block to read

The figure below shows the detail and the meaning of the bytes sent from the Controller to the RWM.



### Answer

The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.

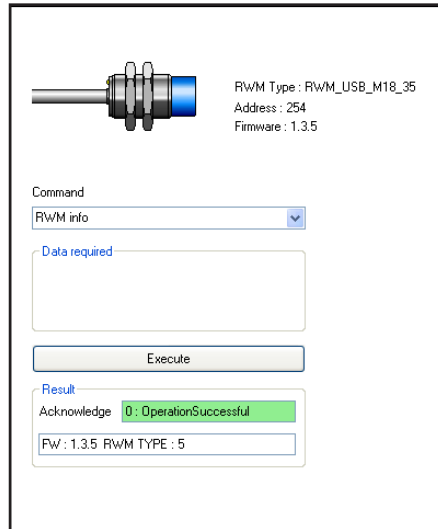




## 34h RWM Info

### Effect of the command

Returns information on the firmware and the type of RWM.

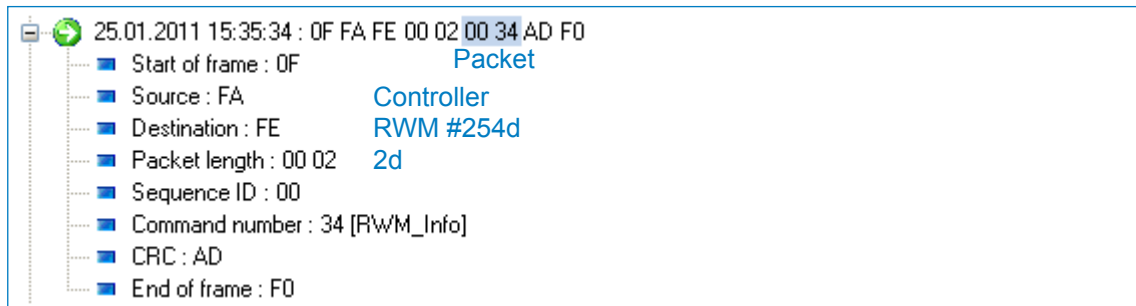


### Command

Data required to write one block in the RWM:

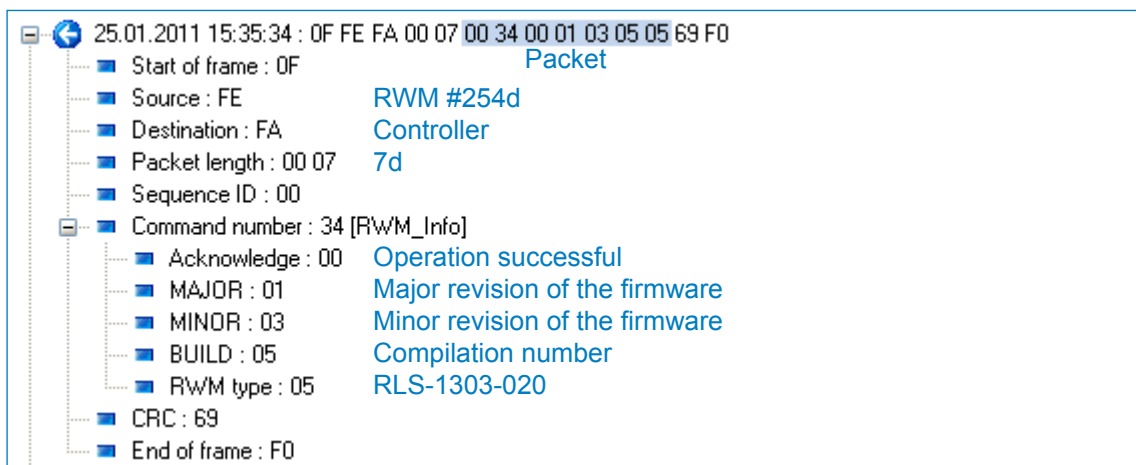
- None

The figure below shows the detail and the meaning of the bytes sent from the Controller to the RWM.



### Answer

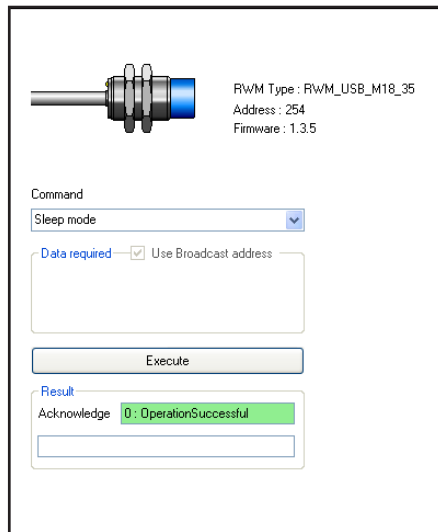
The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.



## 35h Sleep Mode

### Effect of the command

All the RWM decreases its consumption by approximately 50%. The RWM stops to scan the transponders in front of it. The RWM comes out from this mode as soon as a command is sent.



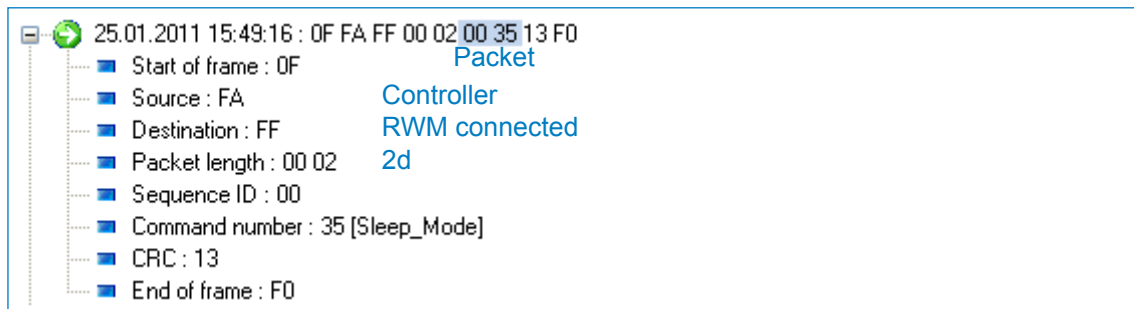
### Command

The broadcast address FFh must be used.

Data required to put RWMs in Sleep Mode:

- None

The figure below shows the detail and the meaning of the bytes sent from the Controller to the RWM.



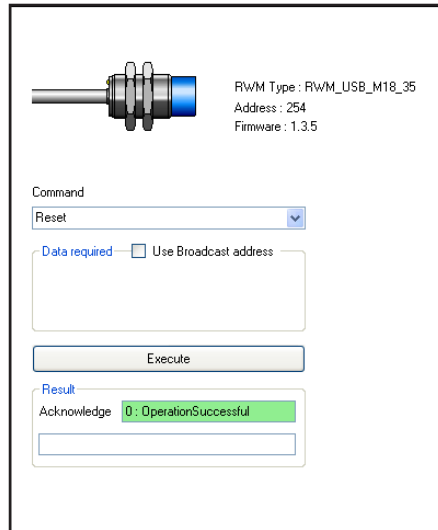
### Answer

There is no answer because of the broadcast mode.

## 36h Reset

### Effect of the command

Restarts the RWM.



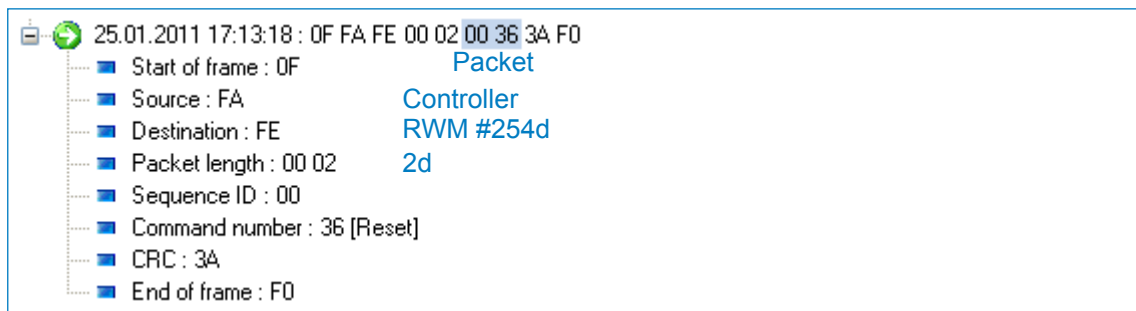
### Command

The broadcast address FFh can be used.

Data required to reset the RWM:

- None

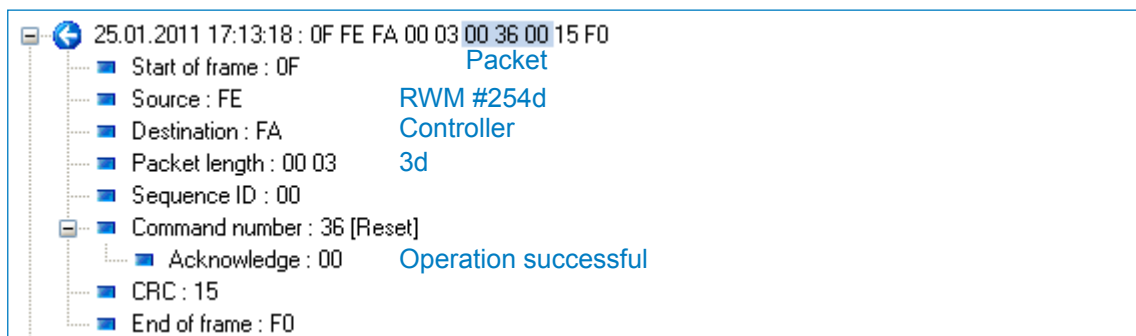
The figure below shows the detail and the meaning of the bytes sent from the Controller to the RWM.



### Answer

The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.

If the broadcast mode has been chosen, there is no answer from the RWM.

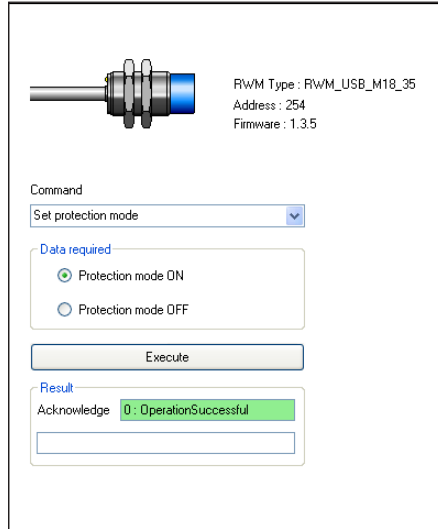


### 3Bh Set Protection Mode

#### Effect of the command

Activates or deactivates the protection mode of the RWM.

The magnetic field of the RWM is maintained as long as the protection mode is activated.

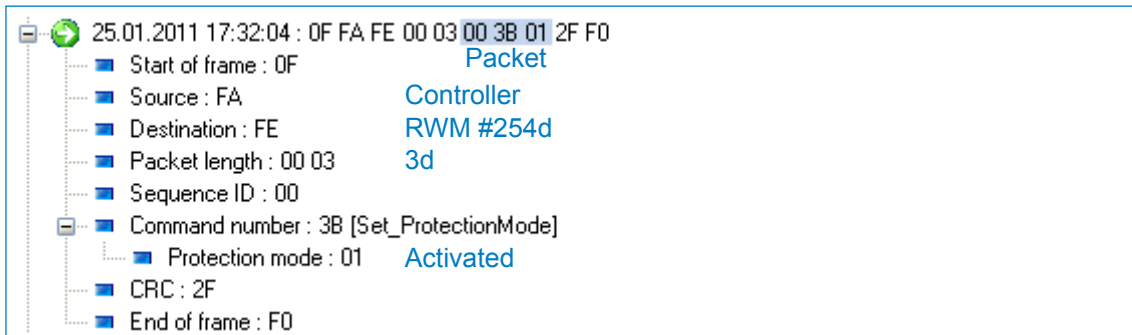


#### Command

Data required to activate or deactivate the protection mode of a RWM:

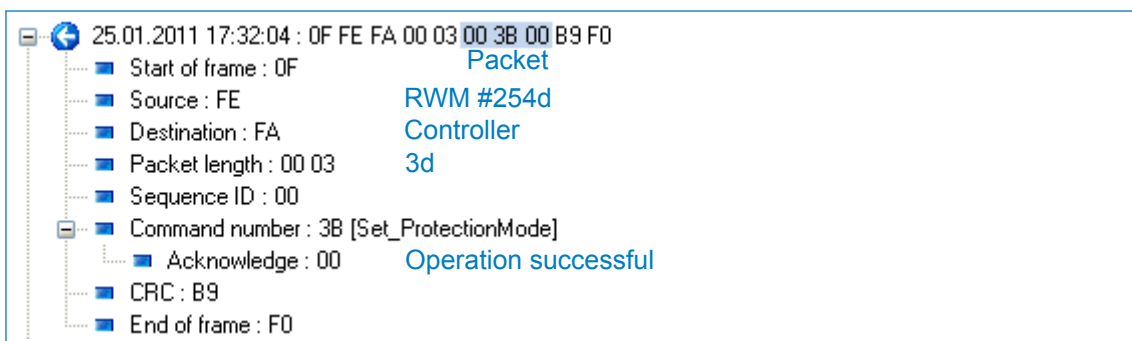
- Status of the protection mode

The figure below shows the detail and the meaning of the bytes sent from the Controller to the RWM.



#### Answer

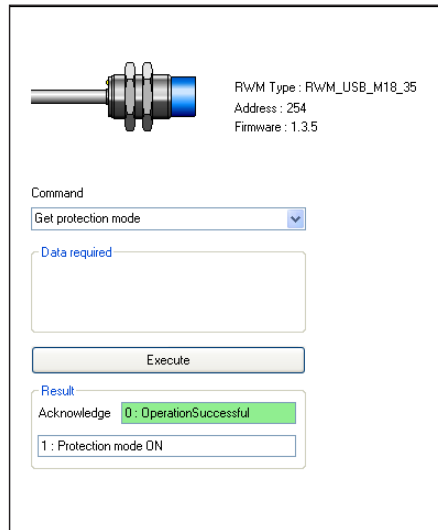
The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.



### 3Ch Get Protection Mode

#### Effect of the command

Returns the status of the protection mode of the RWM

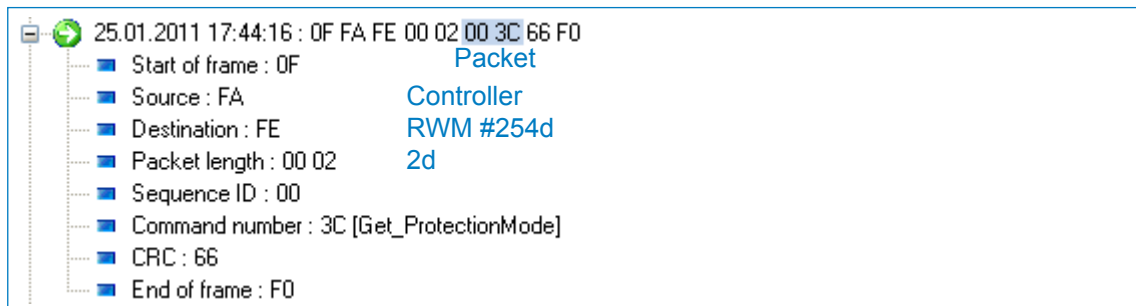


#### Command

Data required to get the status of the protection mode of the RWM:

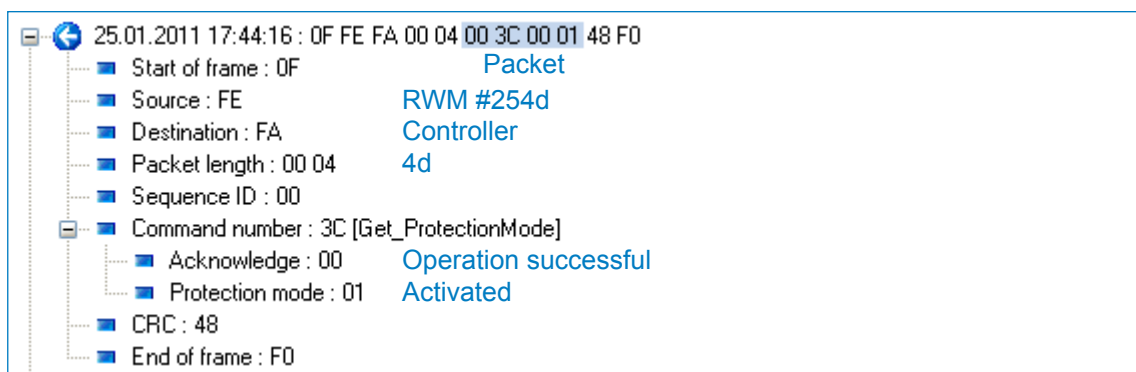
- None

The figure below shows the detail and the meaning of the bytes sent from the Controller to the RWM.



#### Answer

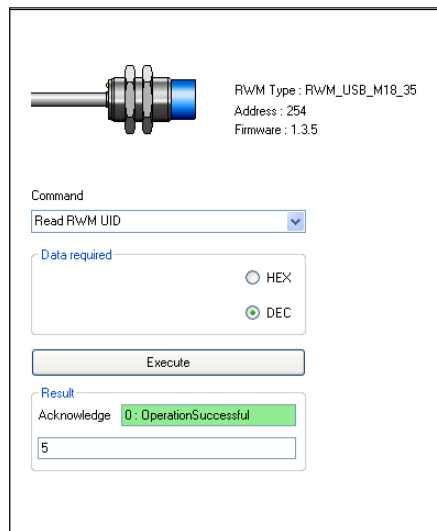
The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.



## 3Fh Read RWM UID

### Effect of the command

Returns the unique identifier (UID) of the RWM.

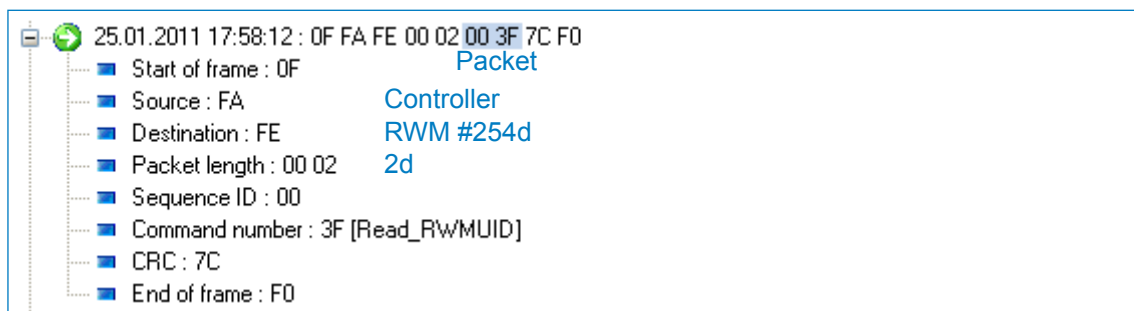


### Command

Data required to read the RWM UID:

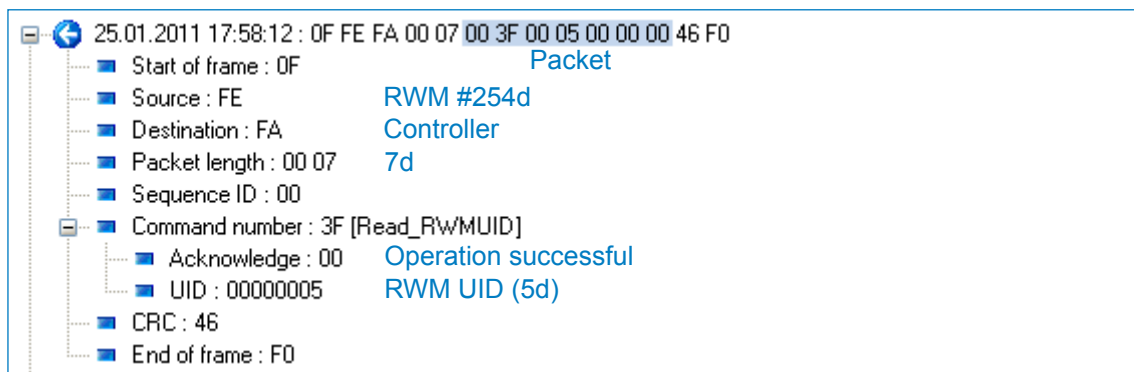
- None

The figure below shows the detail and the meaning of the bytes sent from the Controller to the RWM.



### Answer

The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.

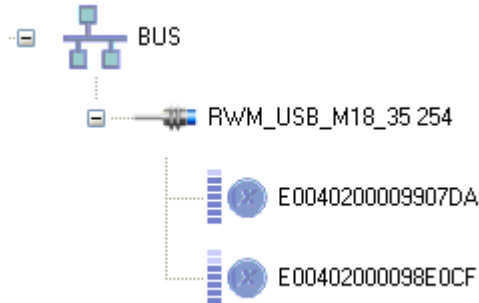


# COMMANDS CONCERNING THE TRANSPONDER (TAG)

## 00h Status

### Description

The RWM is scanned automatically and periodically with the command Status in order to know which are the transponders present.



### Captured packets

When no command is sent, the following packets repeat periodically:

- 25.01.2011 18:22:50 : 0F FE FA 00 1C 00 00 00 02 DA 07 99 00 00 02 04 E0 00 42 04 6E CF E0 98 00 00 02 04 E0 02 42 04 6D 27 F0
- 25.01.2011 18:22:50 : 0F FA FE 00 02 00 00 23 F0

### Structure of the command

25.01.2011 18:22:50 : 0F FA FE 00 02 00 00 23 F0

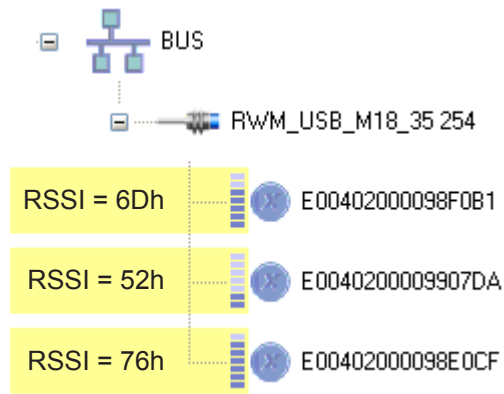
- Start of frame : 0F
- Source : FA Controller (Address 250d)
- Destination : FE RWM #254d
- Packet length : 00 02 2d
- Sequence ID : 00
- Command number : 00 [Status]
- CRC : 23 Cyclic Redundancy Check
- End of frame : F0

### Structure of the answer

25.01.2011 18:22:50 : 0F FE FA 00 1C 00 00 00 02 DA 07 99 00 00 02 04 E0 00 42 04 6E CF E0 98 00 00 02 04 E0 02 42 04 6D 27 F0

- Start of frame : 0F
- Source : FE RWM #254d
- Destination : FA Controller
- Packet length : 00 1C 28d
- Sequence ID : 00
- Command number : 00 [Status]
- Acknowledge : 00 Operation successful
- NBTAG : 02 2 TAGs in front of RWM
  - 00 **First TAG**
    - UID : E0040200009907DA
    - DSFID : 00 Data Storage Format Identifier
    - MEMORG : 42 40 blocks of 32 bit
    - FAB : 04 NXP Semiconductor
    - RSSI : 6E Received Signal Strength Indication
  - 01 **Second TAG**
    - UID : E00402000098EOCF
    - DSFID : 02 Data Storage Format Identifier
    - MEMORG : 42 40 blocks of 32 bit
    - FAB : 04 NXP Semiconductor
    - RSSI : 6D Received Signal Strength Indication
- CRC : 27
- End of frame : F0

RSSI is an indication of the strength of the received signal. These strength is also illustrated by the bar diagram beside the symbol of the transponder in the TreeView.





# Generalities

## Introduction

To understand the various commands of the ConID HF software, it is necessary to know what is the structure of the user memory of the transponder.

The structure of the memory of Contrinex transponders is described below.

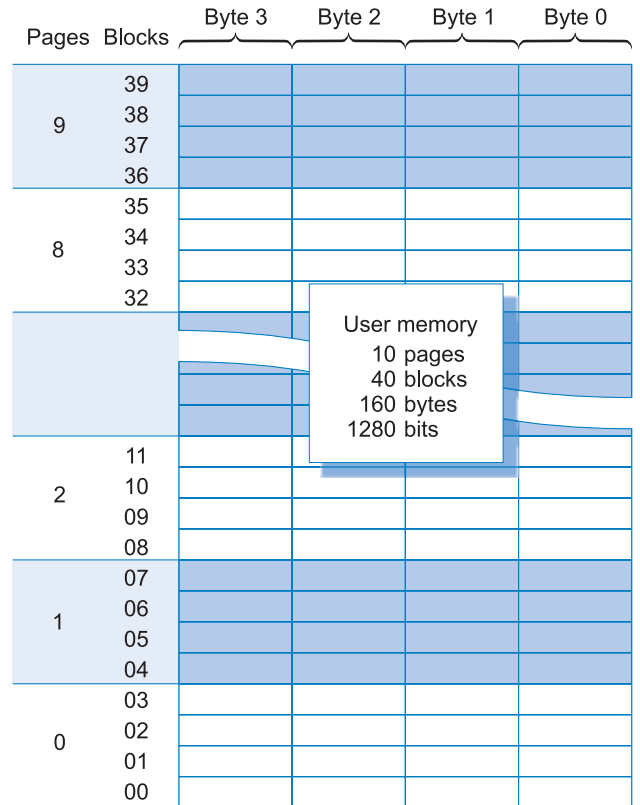
For other transponders, please refer to the specifications of the manufacturer.

## Structure of the user memory

The user part of the EEPROM memory has a capacity of 1280 bits and is organized in 10 pages of 4 blocks, that means 40 blocks of 4 bytes each.

The block is the smallest accessible unit.

The page is the smallest memory unit which can be protected by a password.



## List of the commands other than Status

The list of the commands dedicated to the transponder is accessible in the scroll list "Command". The various commands with their meaning are listed below. Notice that some commands are dedicated to Contrinex transponders or to manufacturers who use SL2 ICS53 I•Code SLI-S transponders.

#	Name	Meaning
00	Status	Returns the list of UIDs of all the transponders in front of the RWM
10	Read	Reads blocks starting from start address
11	Write	Writes blocks of data starting from start address
12	Lock	Protects definitively against writing the selected blocks
13	Stay quiet	Set the concerned transponder in "Quiet state".
14	Select	Set the concerned transponder in "Selected" state.
15	Reset to ready	Set the concerned transponder(s) in "Ready" state.
16	Write AFI	Writes AFI (Application Family Identifier) code
17	Lock AFI	Protects the AFI code definitively against writing
18	Write DSFID	Writes DSFID (Data Storage Format Identifier) code
19	Lock DSFID	Protects the DSFID code definitively against writing
1A	Get Info	Returns the specific characteristics of the transponder
20	Get Random Number	Commands to the transponder to return a random number
21	Set Password	Sends an encrypted password in order to unlock the transponder
22*	Write Password	Modifies the password
23*	Lock Password	Locks, in an irreversible way, the specified password
24*	64 bit Protection	Activates definitively a password of 64 bits
25*	Protect Page	Protects pages in accordance with the desired protection status
26*	Lock Page Protection	Locks, in an irreversible way, the protection conditions of the page
27	Get Protection Status	Returns the protection state of the concerned blocks
28*	Destroy TAG	Deactivates the transponder in an irreversible way

ISO/IEC 15693 standard

For SL2 ICS53 I•Code SLI-S transponders only (Contrinex transponders)

\* A login which is defined by the sequence of the commands "Get Random Number" and "Set Password", is mandatory before this command

# 10h Read

## Effect of the command

Reads blocks (and protection code of each block if option flag is checked) starting from the selected address.

While clicking on the right button of the mouse, it is possible to export data to Excel or to print them.

## Command

The modes Addressed and Selected are possible.

Parameters required to read data in a transponder are:

- the address of the block from which the reading will be carried out (Address block start)
- the number of blocks to read (Number of blocks)
- the option flag. When it is checked, the protection code of each block will be displayed.

The figure below shows the detail and the meaning of the bytes sent from controller to the RWM.

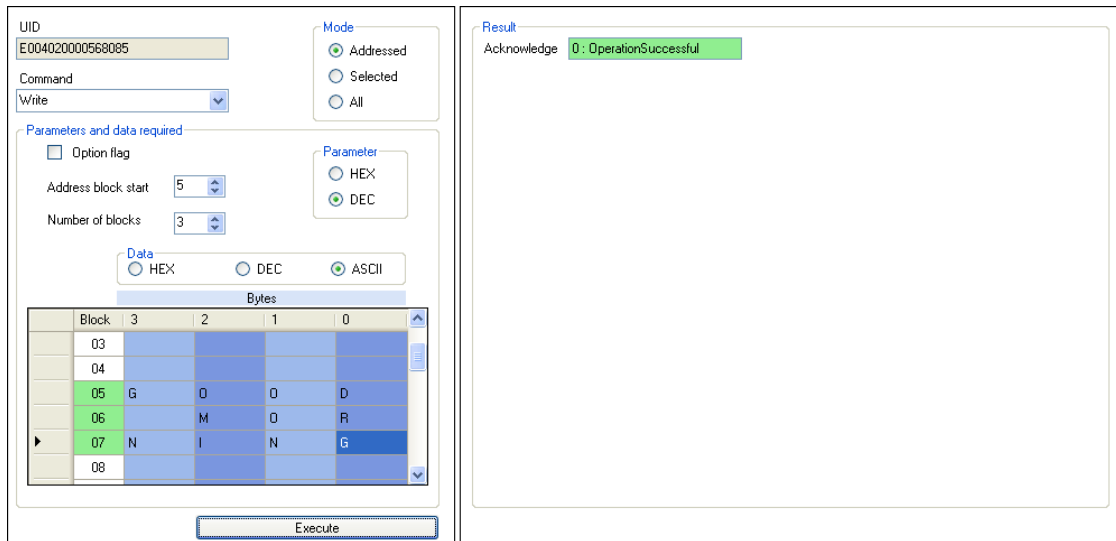
## Answer

The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller. Note that each block is preceded by its protection code.

# 11h Write

## Effect of the command

Writes blocks of data starting from the selected address.



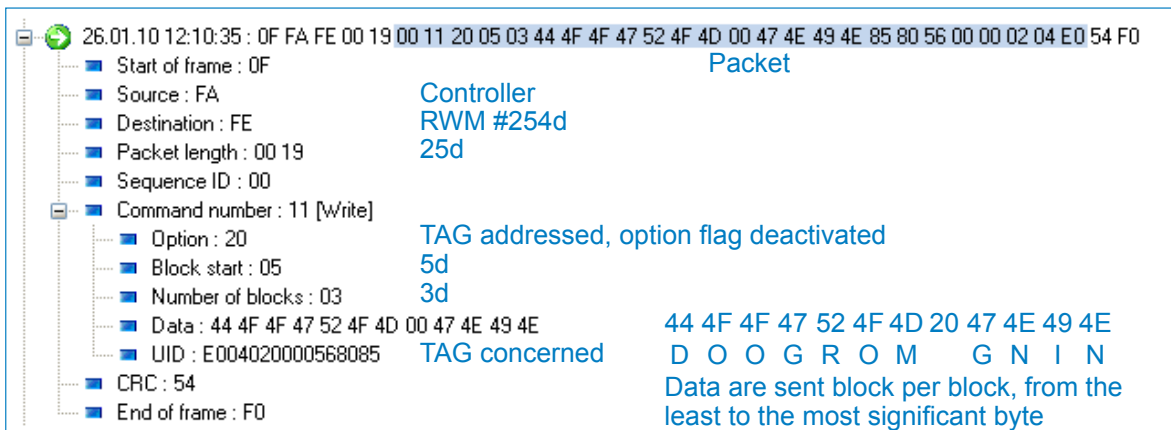
## Command

The three modes (Addressed, Selected, All) are possible.

Parameters required to write data in a transponder are:

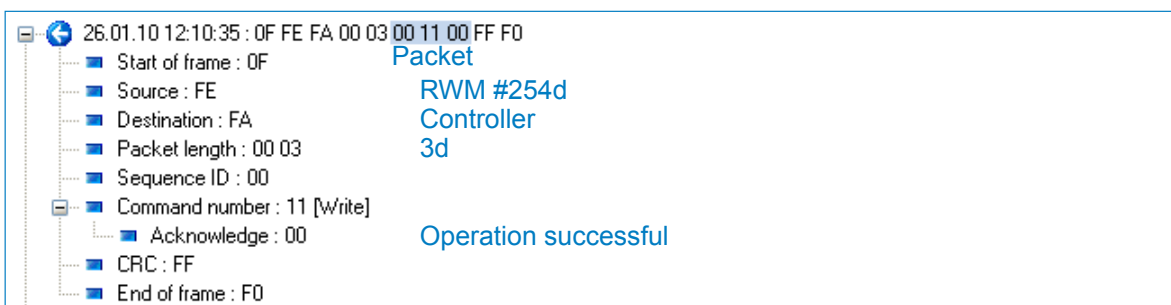
- the address of the block from which the writing will be carried out (Address block start)
- the number of blocks to write (Number of blocks)
- data, entered in the corresponding memory cells
- With Contrinex transponders, the option flag must not be checked. Certain manufacturers (TI for example) require that the option flag be checked in order to perform the writing. Consult the data sheet of the manufacturer to ensure the good progress of the operations.

Figure below shows the detail and the meaning of the bytes sent from Controller to the RWM.



## Answer

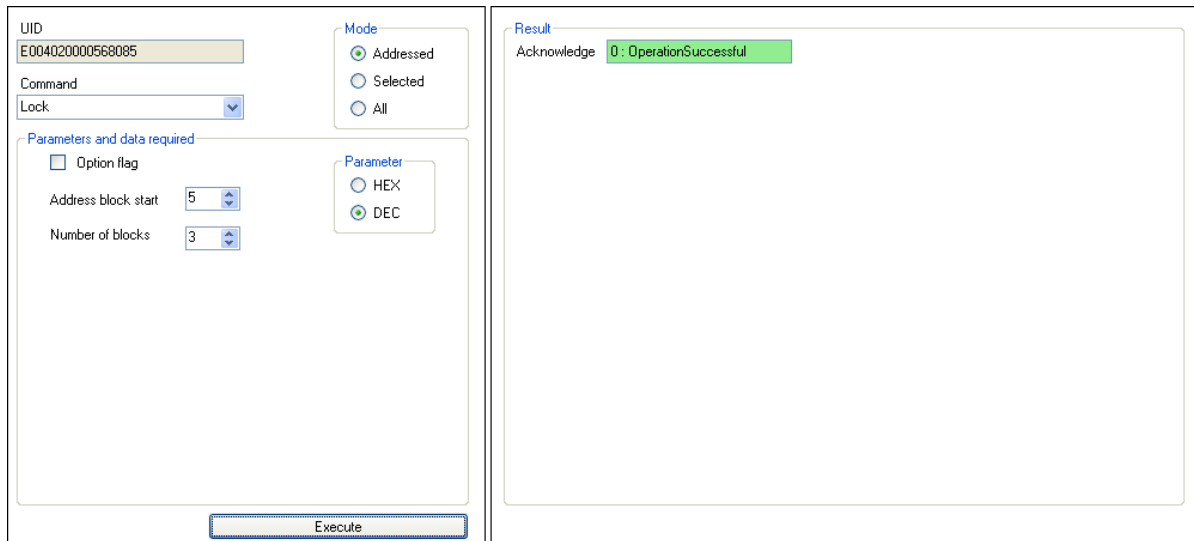
Figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.



# 12h Lock (block)

## Effect of the command

Protects definitively against writing the selected blocks.



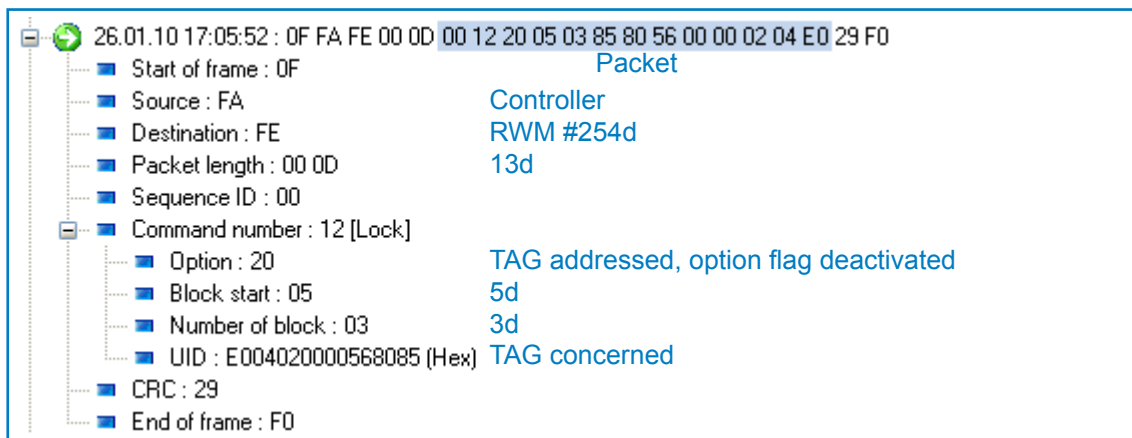
## Command

The three modes (Addressed, Selected, All) are possible.

Parameters required to lock blocks in a transponder are:

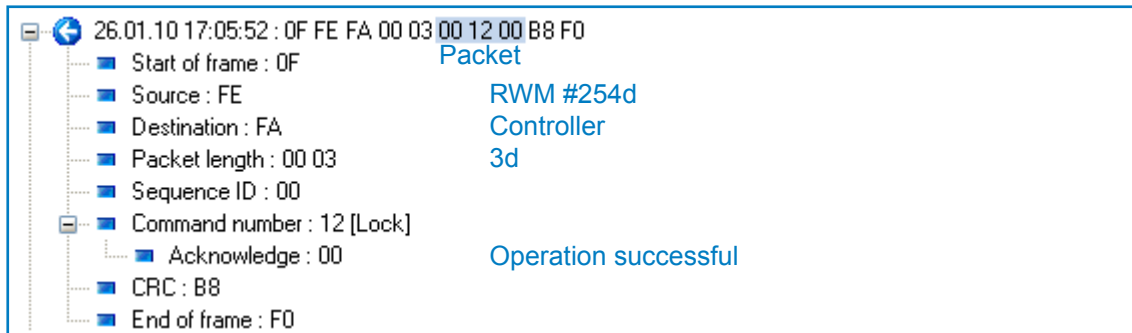
- the address of the block which is the start of the locked area
- the number of blocks to lock (Number of blocks)
- option flag must not be checked.

The figure below shows the detail and the meaning of the bytes sent from Controller to the RWM.



## Answer

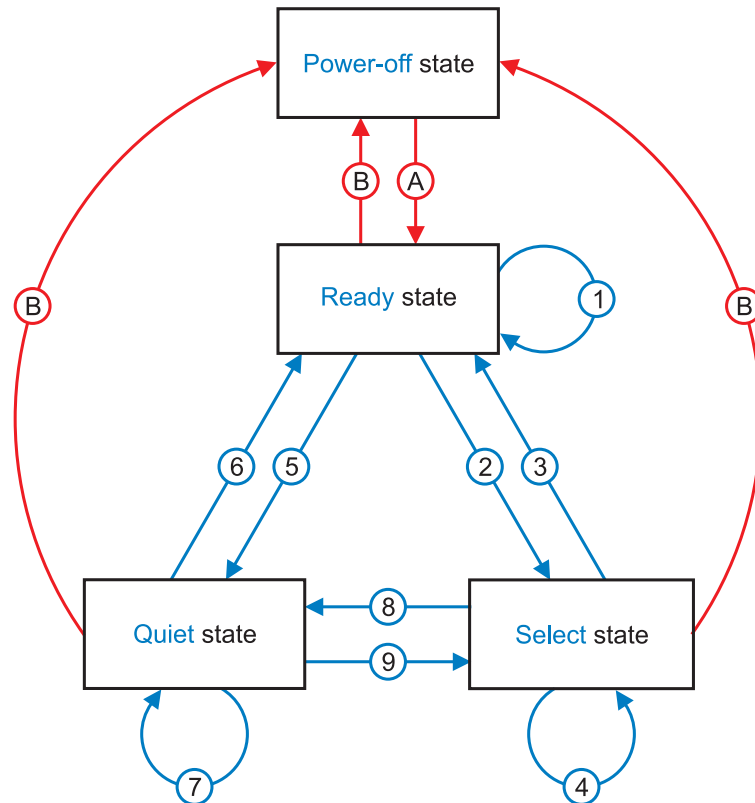
The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.



## Transponder states

Transponder states and transitions between them must be known in order to understand the three following commands:

- 13 Stay quiet
- 14 Select
- 15 Reset to ready

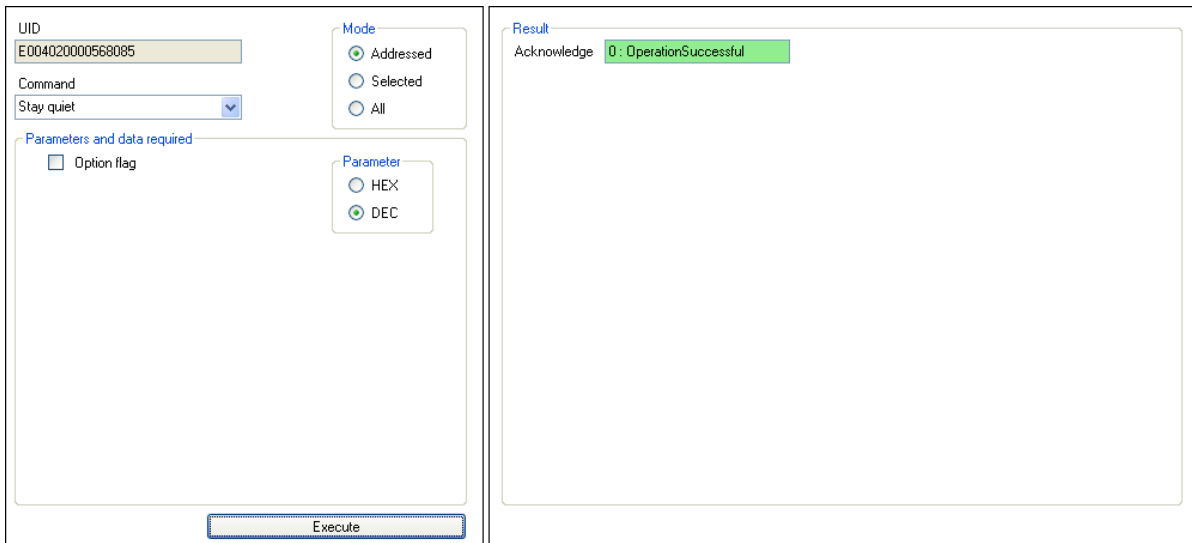


Transition	Description
A	Input in RWM field
B	Output of RWM field
1	Any other command not relating to the selected transponder
2	Select for an addressed transponder (UID mandatory)
3	Reset To Ready for the selected transponder Select for an other addressed transponder (UID mandatory)
4	Any other command
5	Stay Quiet for an addressed transponder (UID mandatory)
6	Reset To Ready
7	Any other command for an addressed transponder (UID mandatory), except Status
8	Stay Quiet: addressed command (UID mandatory) for the selected transponder
9	Select: addressed command (UID mandatory) for the transponder in quiet state

# 13h Stay quiet

## Effect of the command

Set the concerned transponder in the "Quiet state".



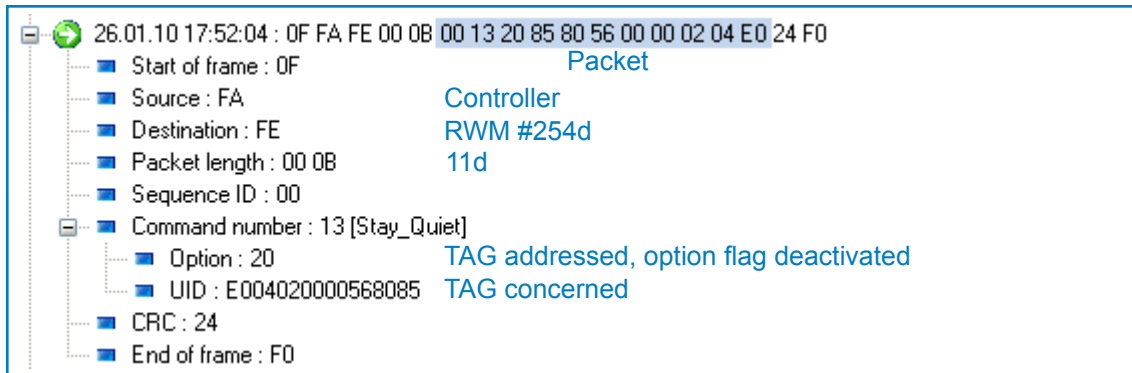
## Command

The transponder must be addressed.

Parameters required to put the transponder in the quiet state are:

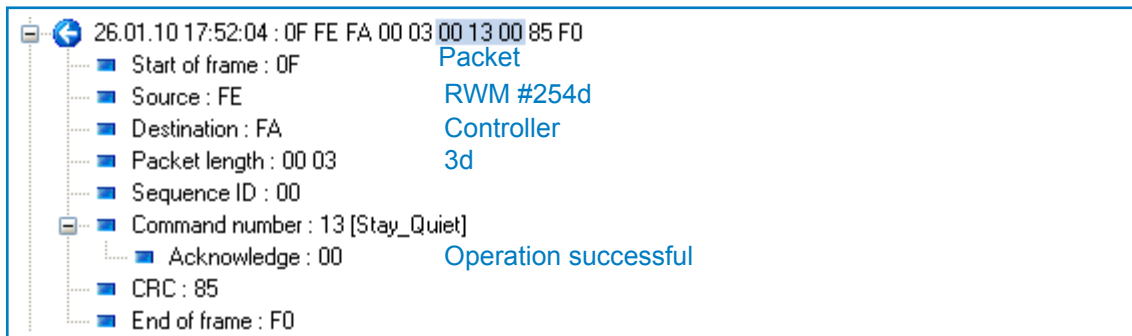
- none
- option flag must not be checked.

The figure below shows the detail and the meaning of the bytes sent from Controller to the RWM.



## Answer

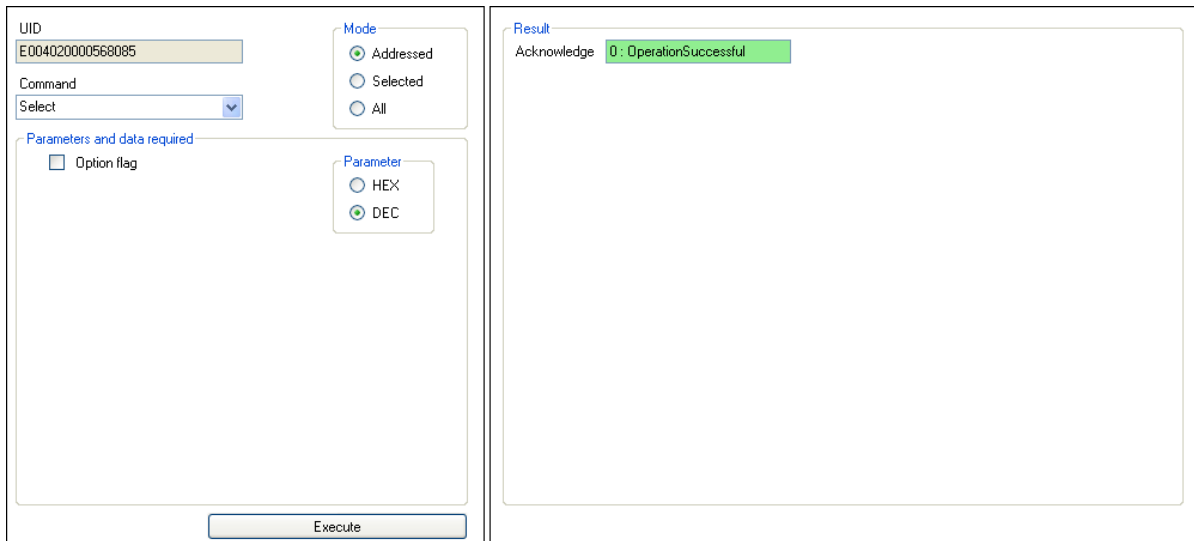
The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.



# 14h Select

## Effect of the command

Set the concerned transponder in "Selected" state.



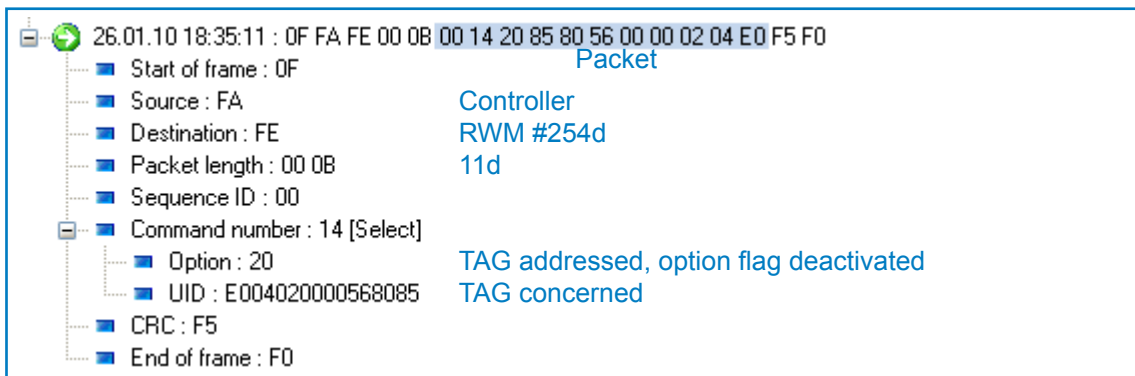
## Command

The transponder must be addressed.

Parameters required to read data in a transponder are:

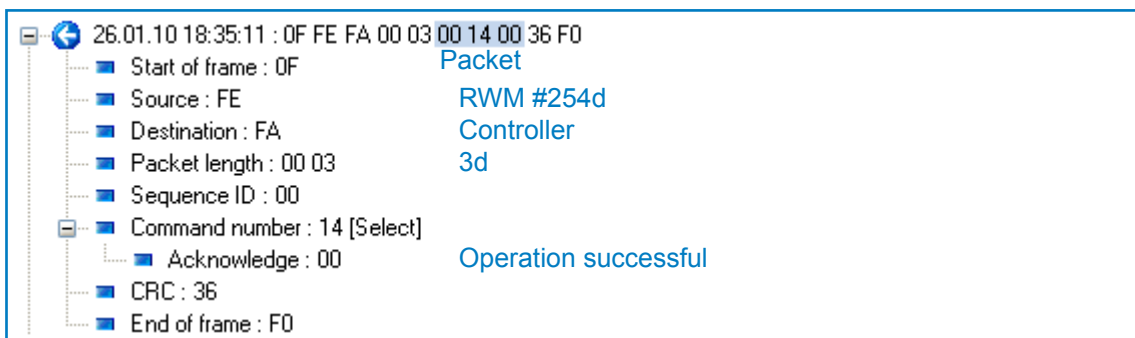
- none
- option flag must not be checked.

The figure below shows the detail and the meaning of the bytes sent from Controller to the RWM.



## Answer

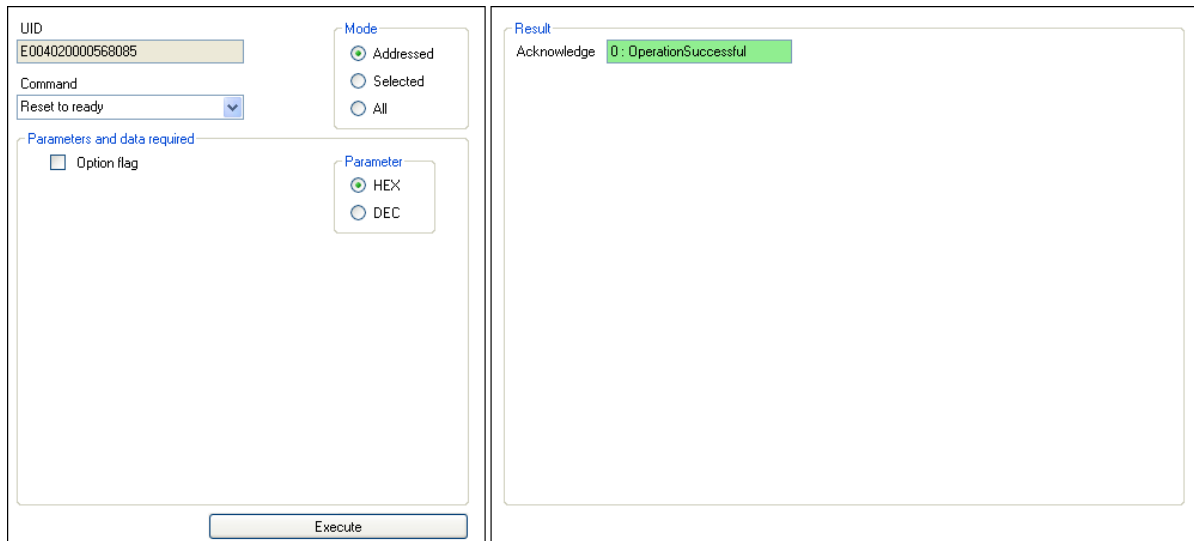
The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.



# 15h Reset To Ready

## Effect of the command

Set the concerned transponder(s) in "Ready" state.



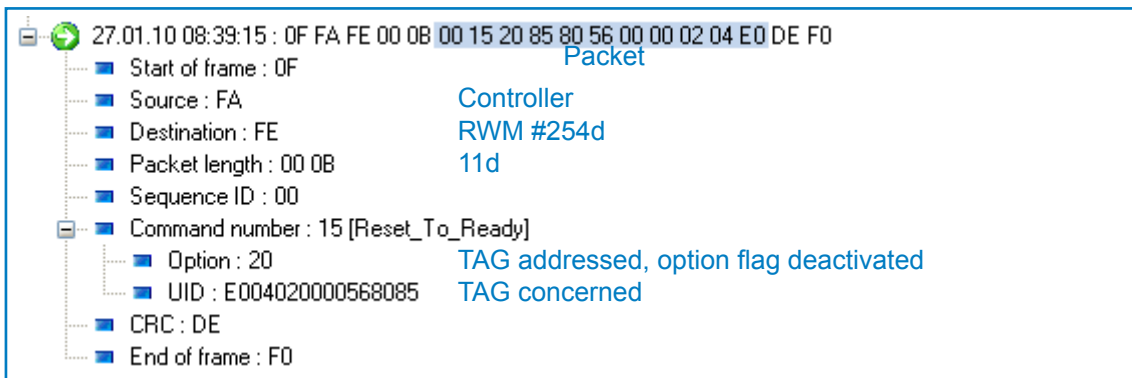
## Command

The three modes (Addressed, Selected, All) are possible.

Parameters required:

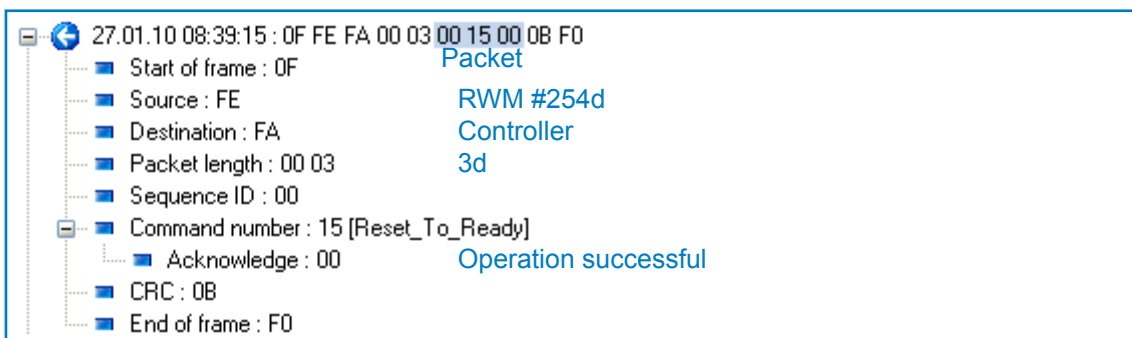
- none
- option flag must not be checked.

The figure below shows the detail and the meaning of the bytes sent from Controller to the RWM.



## Answer

The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.

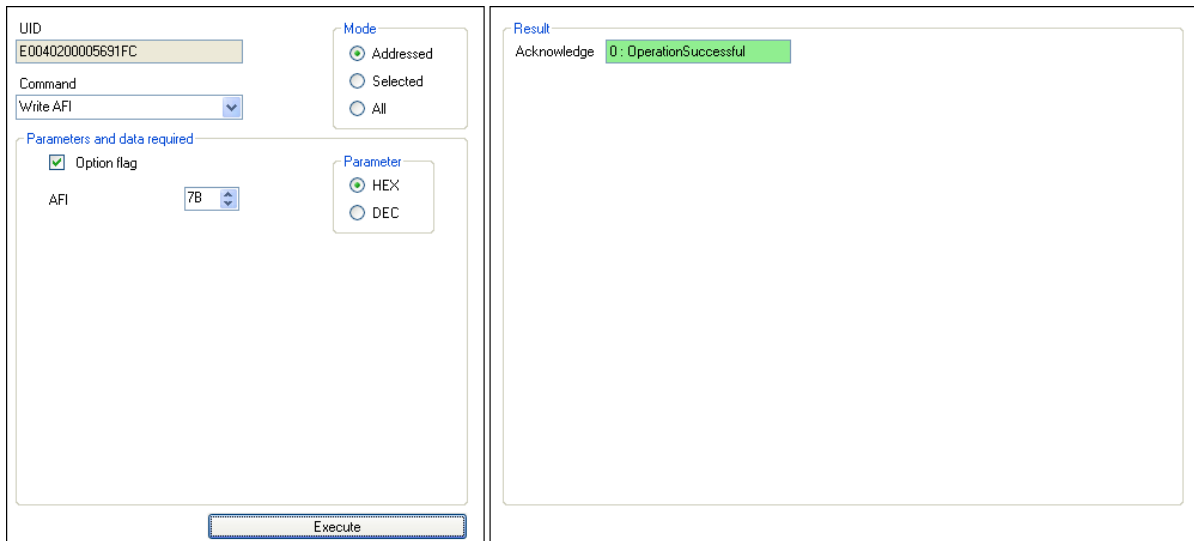




# 16h Write AFI

## Effect of the command

Writes AFI (Application Family Identifier) code.



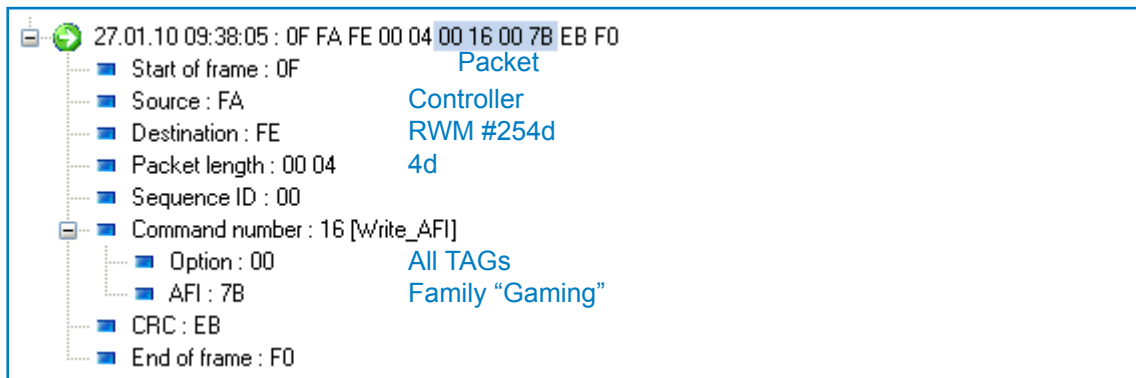
## Command

The three modes (Addressed, Selected, All) are possible.

Parameters required to write AFI (Application Family Identifier) in a transponder are:

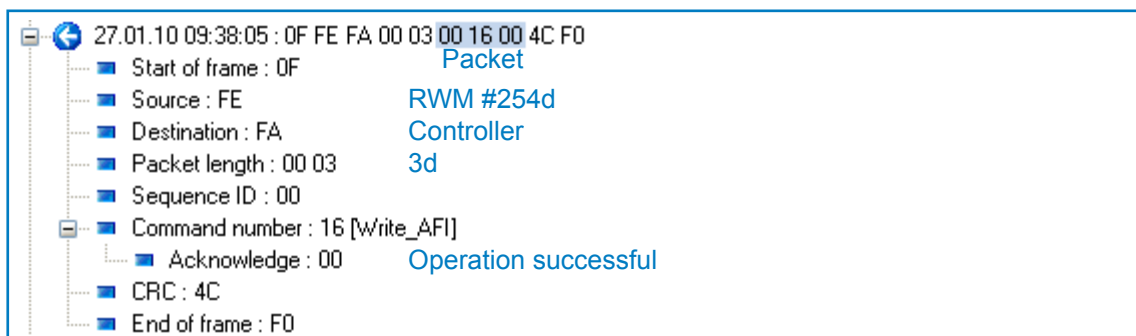
- AFI code (1 byte)
- this command has no effect if the option flag is checked, even if the resulting acknowledge code is 0 (Operation successful)

An acknowledgment 15 (Communication error with the transponder) will be returned if the AFI code is locked. The figure below shows the detail and the meaning of the bytes sent from Controller to the RWM.



## Answer

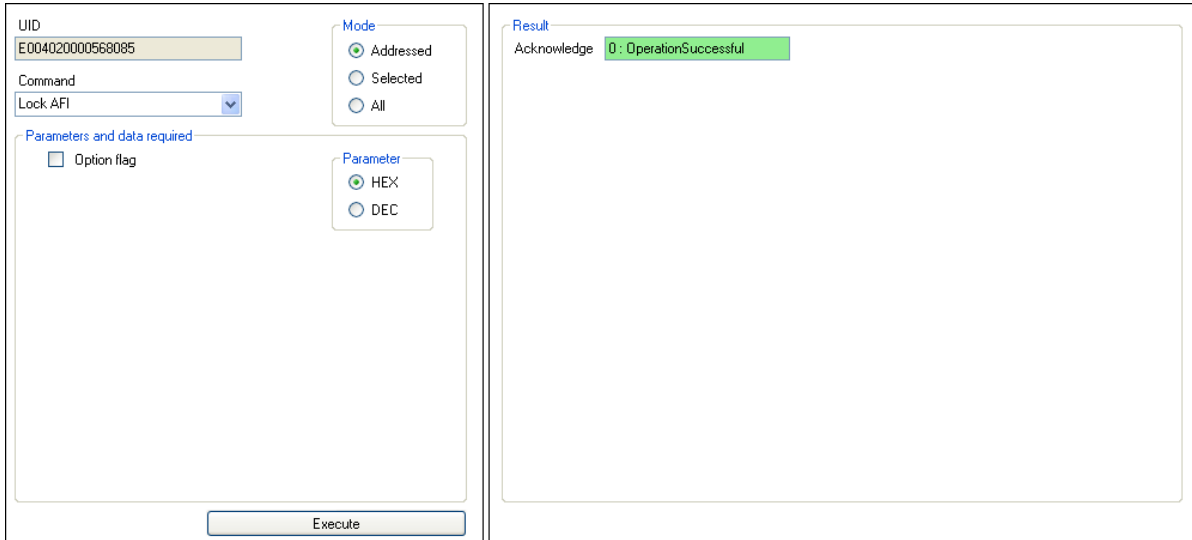
The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.



# 17h Lock AFI

## Effect of the command

Protects definitively the AFI (Application Family Identifier) code against writing.



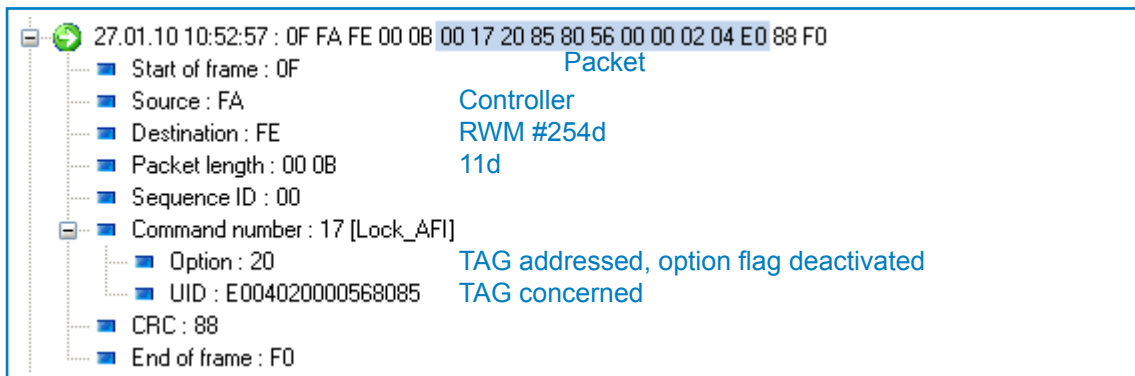
## Command

The three modes (Addressed, Selected, All) are possible.

Parameters required:

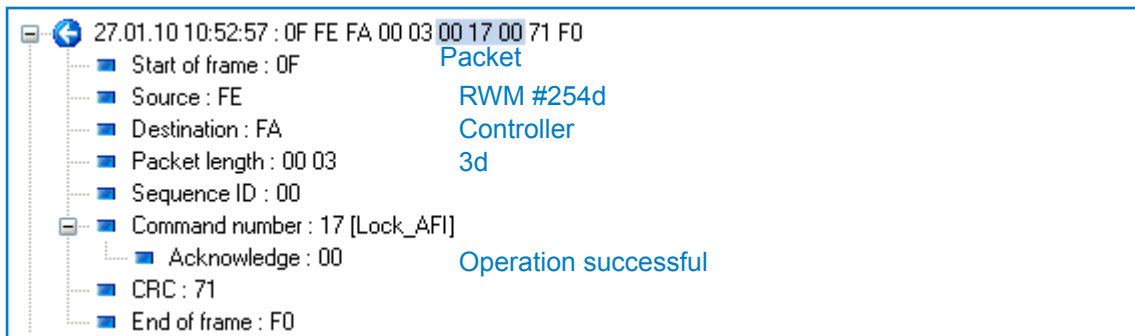
- none
- option flag must not be checked.

The figure below shows the detail and the meaning of the bytes sent from Controller to the RWM.



## Answer

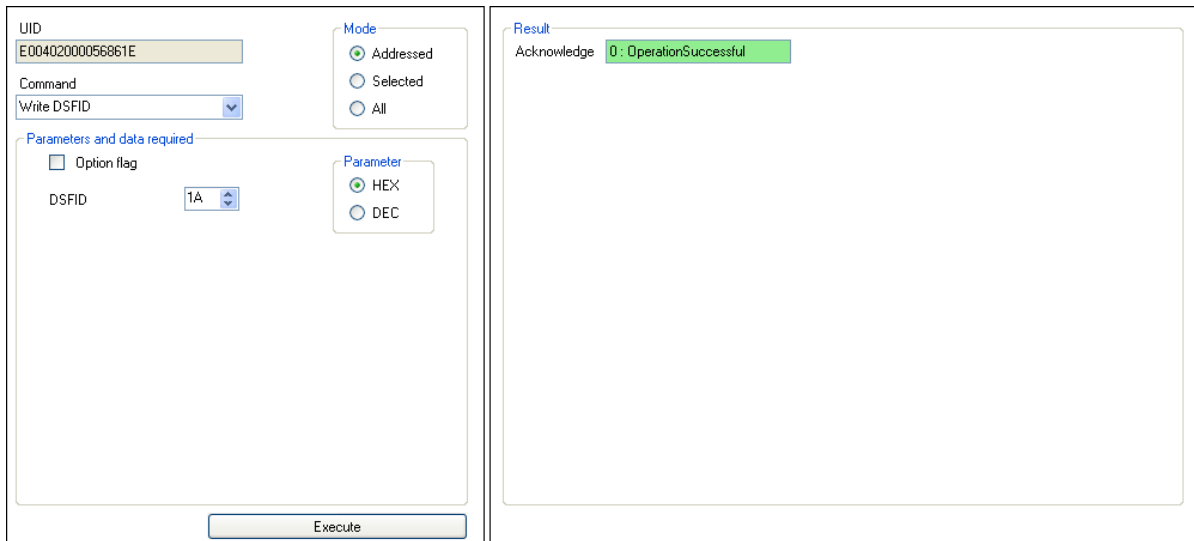
The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.



# 18h Write DSFID

## Effect of the command

Writes DSFID (Data Storage Format Identifier) code.



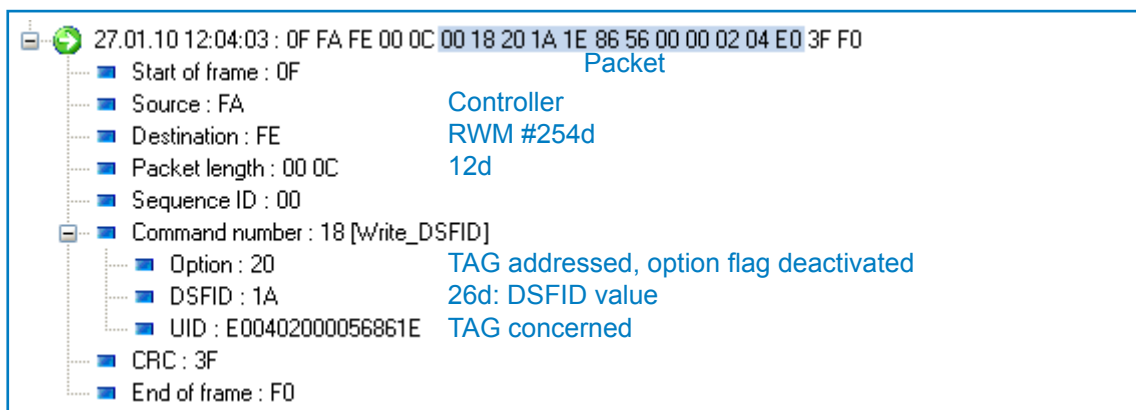
## Command

The three modes (Addressed, Selected, All) are possible.

Parameters required to write AFI (Application Family Identifier) in a transponder are:

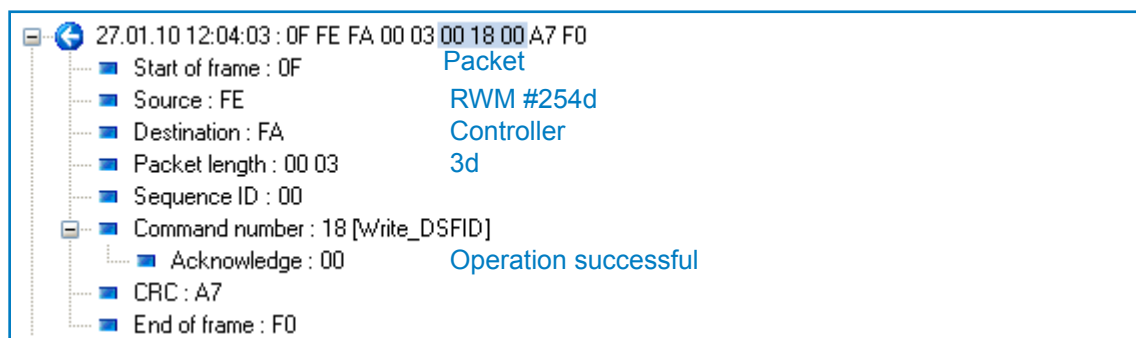
- DSFID code (1 byte)
- option flag must not be checked.

An acknowledgment 15 (Communication error with the transponder) will be returned if the AFI code is locked. The figure below shows the detail and the meaning of the bytes sent from Controller to the RWM.



## Answer

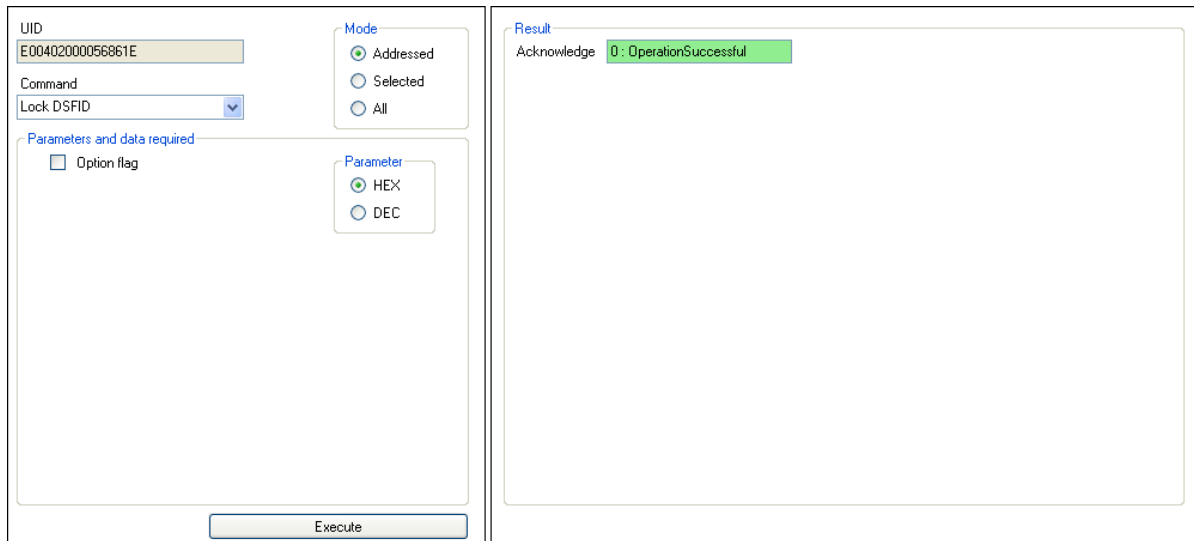
The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.



# 19h Lock DSFID

## Effect of the command

Protects definitively the DSFID code against writing.



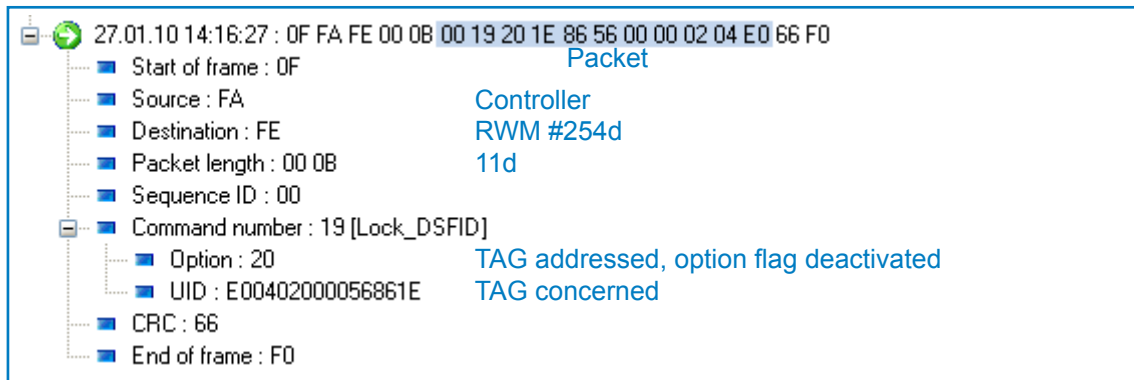
## Command

The three modes (Addressed, Selected, All) are possible.

Parameters required:

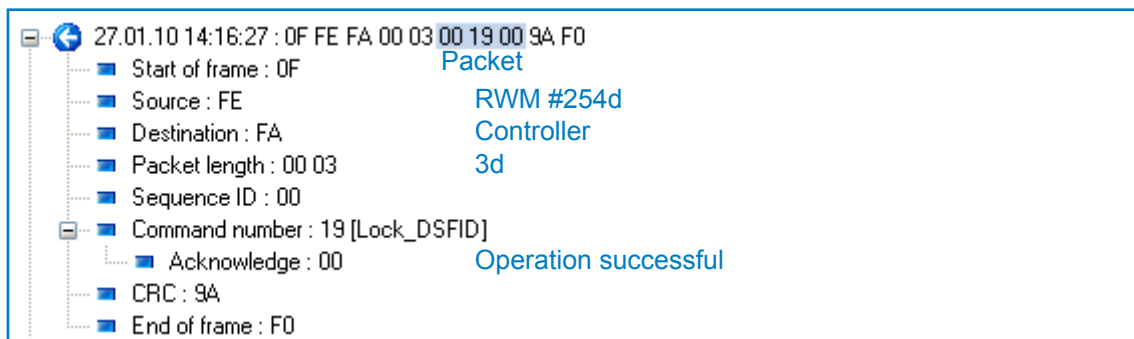
- none
- option flag must not be checked.

The figure below shows the detail and the meaning of the bytes sent from Controller to the RWM.



## Answer

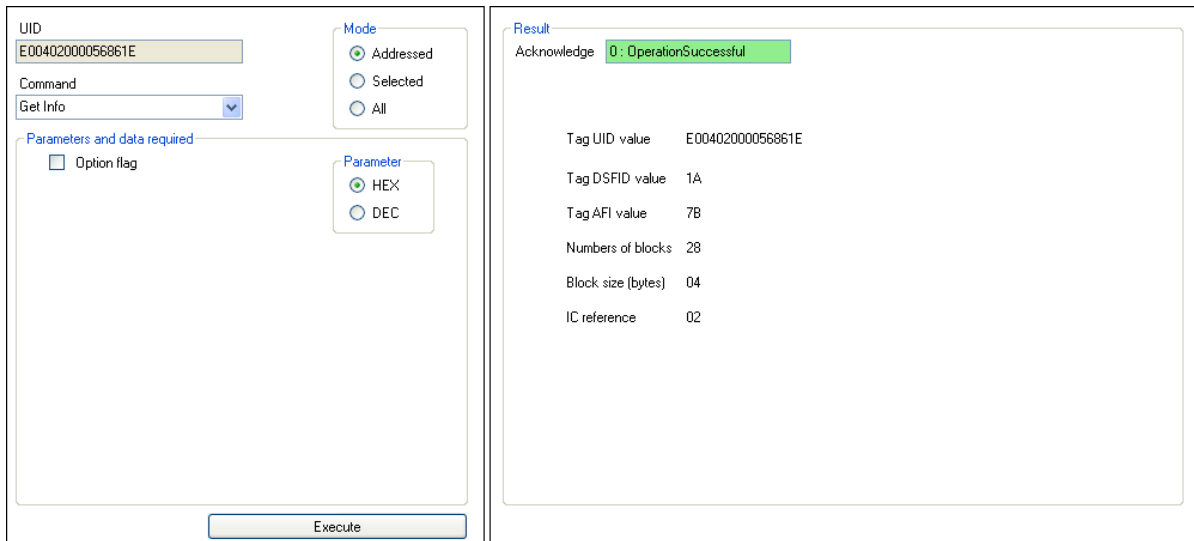
The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.



# 1Ah Get Info

## Effect of the command

Returns the specific characteristics of the transponder



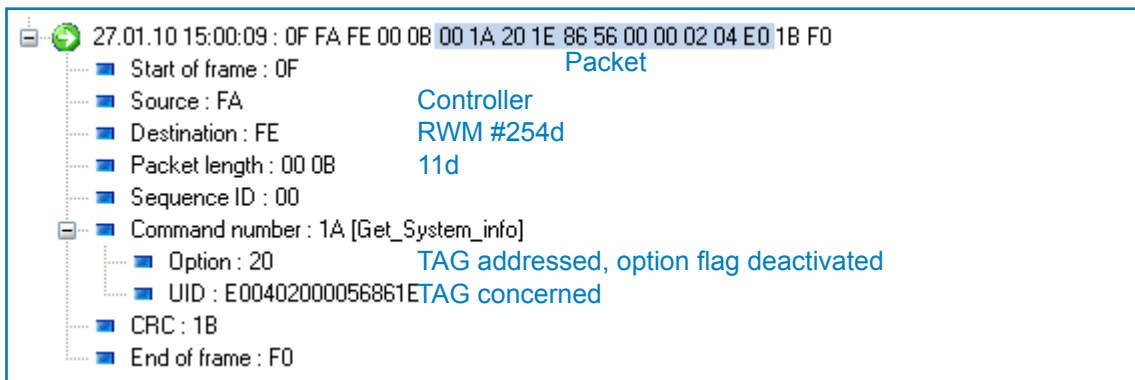
## Command

The modes Addressed and Selected are possible.

Parameters required:

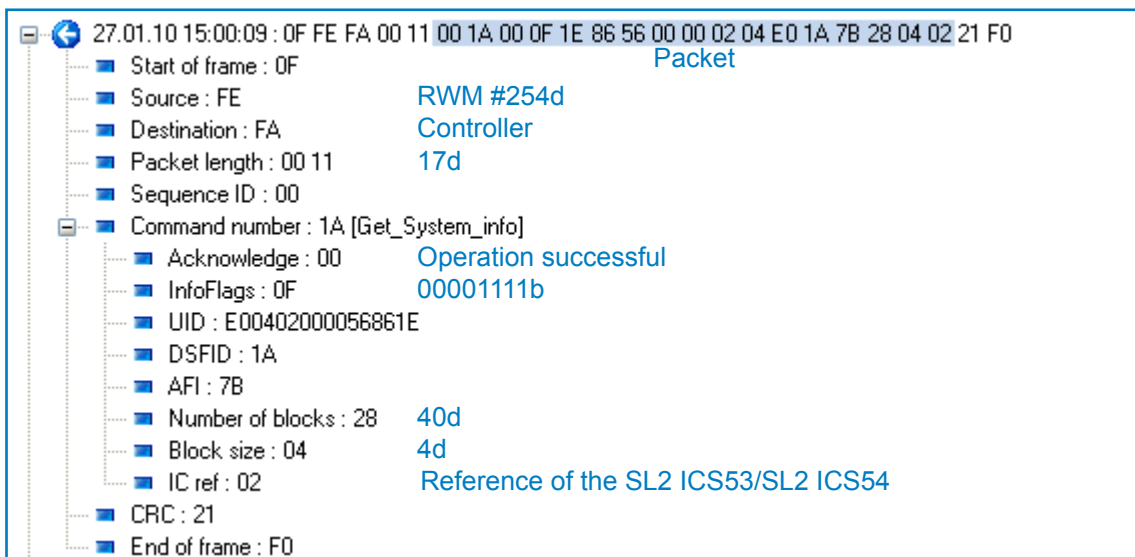
- none
- option flag must not be checked.

The figure below shows the detail and the meaning of the bytes sent from Controller to the RWM.



## Answer

The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.



## 20h Get Random Number

### Effect of the command

Commands to the transponder to return a random number

The screenshot shows a software interface for sending a command to a transponder. On the left, there are fields for UID (E00402000056861E), Command (Get Random Number), and Mode (Addressed, Selected, All). Below these are checkboxes for 'Option flag' and 'Parameter' (HEX, DEC). An 'Execute' button is at the bottom. On the right, a 'Result' box shows 'Acknowledge: 0: OperationSuccessful'.

### Comment

Before sending this command, the protection mode of the corresponding RWM must be enabled.

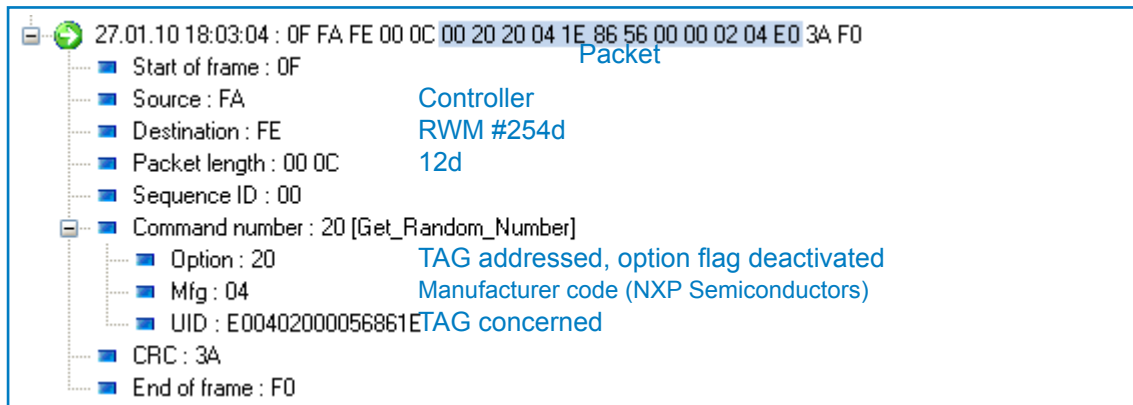
### Command

The modes Addressed and Selected are possible.

Parameters required:

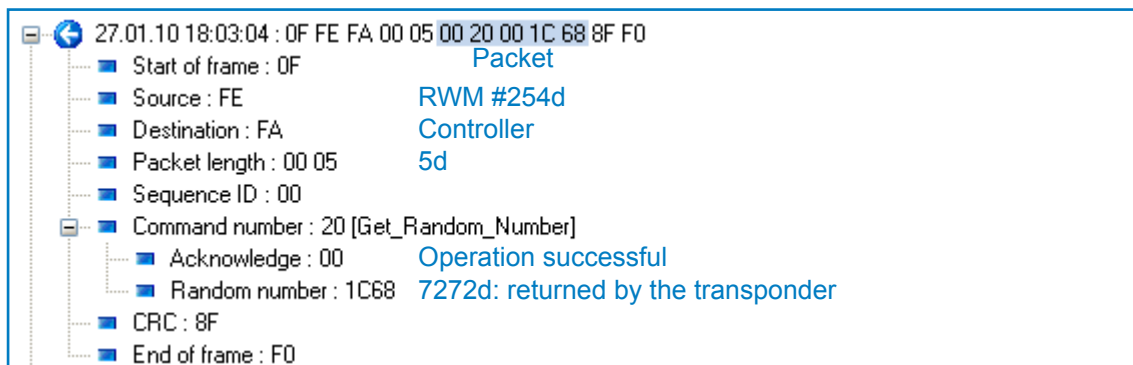
- none
- option flag must not be checked.

The figure below shows the detail and the meaning of the bytes sent from Controller to the RWM.



### Answer

The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.



## 21h Set Password

### Effect of the command

Sends the encrypted password to the transponder in order to unlock it.

UID: E00402000056861E

Command: Set Password

Mode:  Addressed,  Selected,  All

Parameters and data required:  Option flag

Parameter:  HEX,  DEC

I-CODE SLI-S Security

PW ID: 01: Read

Password: 0

Get Random Number: 51B4

XOR PW: 51B451B4

Execute

Result: Acknowledge 0: OperationSuccessful

### Comment

Before sending this command, the protection mode of the corresponding RWM must be enabled.

### Command

The modes Addressed and Selected are possible.

Parameters required:

- none
- option flag must not be checked.

The figure below shows the detail and the meaning of the bytes sent from Controller to the RWM.

28.01.10 08:12:57 : 0F FA FE 00 09 00 21 10 04 01 B4 51 B4 51 8A F0  
Packet

- Start of frame : 0F
- Source : FA Controller
- Destination : FE RWM #8d
- Packet length : 00 09 9d
- Sequence ID : 00
- Command number : 21 [Set\_Password]
- Option : 10 TAG selected, option flag deactivated
- Mfg : 04 Manufacturer code (NXP Semiconductors)
- PWID : 01 Read password
- PW : B451B451 Encrypted read password
- CRC : 8A
- End of frame : F0

### Answer

The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.

28.01.10 08:12:57 : 0F FE FA 00 03 00 21 00 2C F0  
Packet

- Start of frame : 0F
- Source : FE RWM #254d
- Destination : FA Controller
- Packet length : 00 03 3d
- Sequence ID : 00
- Command number : 21 [Set\_Password]
- Acknowledge : 00 Operation successful
- CRC : 2C
- End of frame : F0

## 22h Write Password

### Effect of the command

Allows to modify the password.

UID: E00402000056861E  
Command: Write Password  
Mode:  Addressed,  Selected,  All  
Parameters and data required:  Option flag  
Parameter:  HEX,  DEC  
I-CODE SLI-S Security: PW ID: 01: Read, Password: CAFE  
Execute

Result: Acknowledge 0: OperationSuccessful

### Comment

A login is mandatory before this command and the protection mode of the RWM must be enabled.

### Command

The modes Addressed and Selected are possible.

Parameters required:

- Password identifier (01: Read, 02: Write, 08: Destroy TAG)
- New password (up to 8 HEX digits)
- option flag must not be checked.

The figure below shows the detail and the meaning of the bytes sent from Controller to the RWM.

```
28.01.10 10:37:02 : 0F FA FE 00 11 00 22 20 04 01 FE CA 00 00 1E 86 56 00 00 02 04 E0 48 F0
  Start of frame : 0F
  Source : FA Controller
  Destination : FE RWM #8d
  Packet length : 00 11 17d
  Sequence ID : 00
  Command number : 22 [Write_Password]
    Option : 20 TAG addressed, option flag deactivated
    Mfg : 04 Manufacturer code (NXP Semiconductors)
    PWID : 01 Read password
    PW : FECA0000 New password
    UID : E00402000056861E TAG concerned
  CRC : 48
  End of frame : F0
```

### Answer

The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.

```
28.01.10 10:37:02 : 0F FE FA 00 03 00 22 00 6B F0
  Start of frame : 0F
  Source : FE RWM #254d
  Destination : FA Controller
  Packet length : 00 03 3d
  Sequence ID : 00
  Command number : 22 [Write_Password]
    Acknowledge : 00 Operation successful
  CRC : 6B
  End of frame : F0
```



## 23h Lock Password

### Effect of the command

Locks, in an irreversible way, the specified password.

The screenshot shows a software interface for sending a command to a device. On the left, the 'UID' field contains 'E00402000056861E'. The 'Command' dropdown is set to 'Lock Password'. Under 'Mode', the 'Addressed' radio button is selected. Under 'Parameter', the 'HEX' radio button is selected. There is an 'Option flag' checkbox which is unchecked. Below that, the 'I-CODE SLI-S Security' section has a 'PW ID' dropdown set to '01: Read'. An 'Execute' button is at the bottom. On the right, the 'Result' section shows 'Acknowledge 0: OperationSuccessful' in a green box.

### Comment

A login is mandatory before this command and the protection mode of the RWM must be enabled.

### Command

The modes Addressed and Selected are possible.

Parameters required:

- Password identifier (01: Read, 02: Write, 08: Destroy TAG)
- option flag must not be checked.

The figure below shows the detail and the meaning of the bytes sent from Controller to the RWM.

The figure shows a Wireshark packet capture of a Lock Password command. The packet is 13 bytes long. The details pane shows the following information:

- Start of frame : 0F
- Source : FA Controller
- Destination : FE RWM #254d
- Packet length : 00 0D 13d
- Sequence ID : 00
- Command number : 23 [Lock\_Password]
- Option : 20 TAG selected, option flag deactivated
- Mfg : 04 Manufacturer code (NXP Semiconductors)
- PwID : 01 Read password
- UID : E00402000056861E TAG concerned
- CRC : 3F
- End of frame : F0

### Answer

The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.

The figure shows a Wireshark packet capture of the Acknowledge response. The packet is 3 bytes long. The details pane shows the following information:

- Start of frame : 0F
- Source : FE RWM #254d
- Destination : FA Controller
- Packet length : 00 03 3d
- Sequence ID : 00
- Command number : 23 [Lock\_Password]
- Acknowledge : 00 Operation successful
- CRC : 56
- End of frame : F0

## 24h 64 bit Password Protection

### Effect of the command

Activates definitively a password of 64 bits made up of the read and write passwords.

The screenshot shows a configuration window for a 64-bit password protection command. On the left, the 'UID' field contains 'E00402000056861E'. The 'Command' dropdown is set to '64 bits protection'. Under 'Mode', the 'Addressed' radio button is selected. Under 'Parameter', the 'HEX' radio button is selected. There is an 'Option flag' checkbox which is unchecked. A 'Parameters and data required' section is empty. At the bottom left is an 'Execute' button. On the right, the 'Result' section shows 'Acknowledge: 0: OperationSuccessful' in a green box.

### Comment

A login is mandatory before this command and the protection mode of the RWM must be enabled.  
64 bit mode is irreversible.

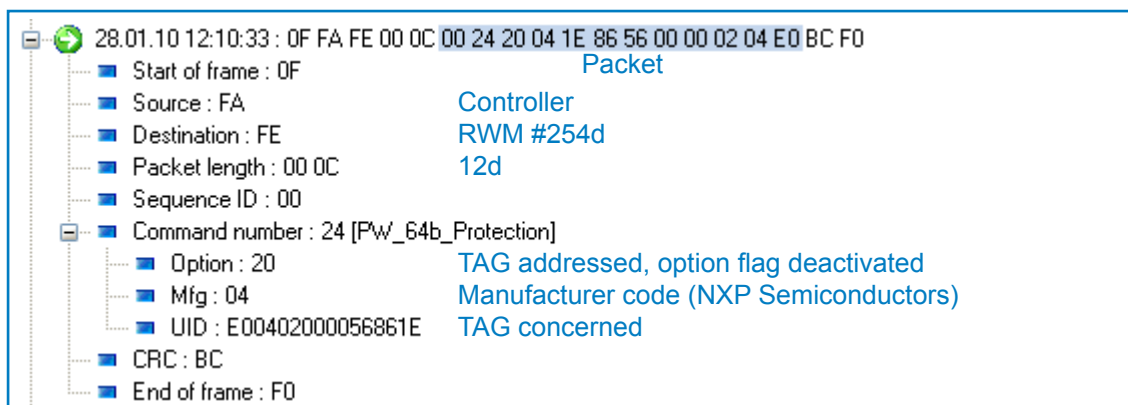
### Command

The modes Addressed and Selected are possible.

Parameters required:

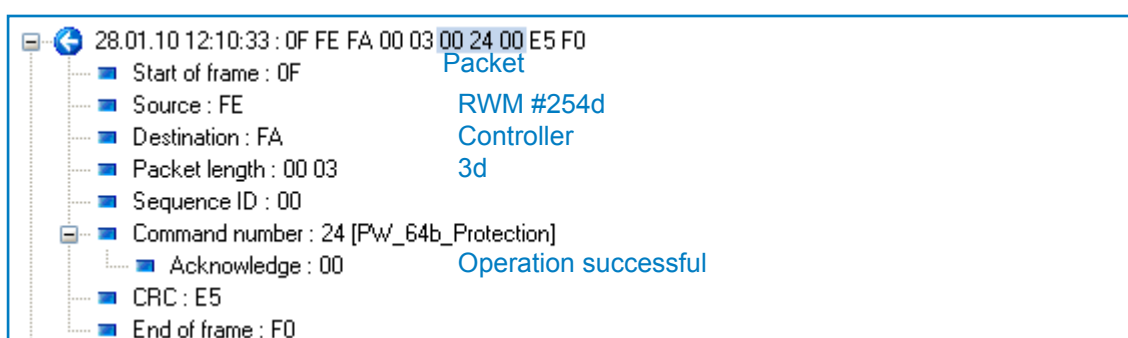
- None
- option flag must not be checked.

The figure below shows the detail and the meaning of the bytes sent from Controller to the RWM.



### Answer

The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.



## 25h Protect Page

### Effect of the command

Protects the specified pages in accordance with the desired protection status.

UID E004020000568267 Command Protect Page Parameters and data required <input type="checkbox"/> Option flag Parameter <input checked="" type="radio"/> HEX <input type="radio"/> DEC I-CODE SLI-S Security Protect : 01: R and 'W by R_PW protected Page number : 1 Execute	Result Acknowledge 0: OperationSuccessful <table border="1"> <thead> <tr> <th>Code</th> <th>Type of protection</th> </tr> </thead> <tbody> <tr> <td>00</td> <td>No protection (public)</td> </tr> <tr> <td>01</td> <td>Read and Write protection by the Read password</td> </tr> <tr> <td>10</td> <td>Write protection by the Write password</td> </tr> <tr> <td>11</td> <td>Read protection by the Read password and Write protection by the Write password</td> </tr> </tbody> </table>	Code	Type of protection	00	No protection (public)	01	Read and Write protection by the Read password	10	Write protection by the Write password	11	Read protection by the Read password and Write protection by the Write password
Code	Type of protection										
00	No protection (public)										
01	Read and Write protection by the Read password										
10	Write protection by the Write password										
11	Read protection by the Read password and Write protection by the Write password										

### Comment

A login is mandatory before this command and the protection mode of the RWM must be enabled.

### Command

The modes Addressed and Selected are possible.

Parameters required:

- Type of protection
- option flag must not be checked.

The figure below shows the detail and the meaning of the bytes sent from Controller to the RWM.

```

28.01.10 14:29:09 : 0F FA FE 00 0E 00 25 20 04 01 01 67 82 56 00 00 02 04 E0 F8 F0
Packet
  Start of frame : 0F
  Source : FA Controller
  Destination : FE RWM #254d
  Packet length : 00 0E 14d
  Sequence ID : 00
  Command number : 25 [Protect_Page]
    Option : 20 TAG selected, option flag deactivated
    Mfg : 04 Manufacturer code (NXP Semiconductors)
    PgNum : 01 Page number 1
    Prot Status : 01 R and W by R_PW protected
    UID : E004020000568267 TAG concerned
  CRC : F8
  End of frame : F0
  
```

### Answer

The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.

```

28.01.10 14:29:09 : 0F FE FA 00 03 00 25 00 2D F0
Packet
  Start of frame : 0F
  Source : FE RWM #254d
  Destination : FA Controller
  Packet length : 00 03 3d
  Sequence ID : 00
  Command number : 25 [Protect_Page]
    Acknowledge : 00 Operation successful
  CRC : 2D
  End of frame : F0
  
```

## 26h Lock Page Protection Condition

### Effect of the command

Locks, in an irreversible way, the protection conditions of the page concerned.

The screenshot shows the I-CODE SLI-S Security configuration window. On the left, the 'UID' field contains 'E004020000568267'. The 'Command' dropdown is set to 'Lock Page Protection'. Under 'Parameters and data required', the 'Option flag' checkbox is unchecked. The 'Mode' section has 'Addressed' selected. The 'Parameter' section has 'HEX' selected. The 'Page number' dropdown is set to '1'. An 'Execute' button is at the bottom. On the right, the 'Result' window shows 'Acknowledge: 0: OperationSuccessful'.

### Comment

A login is mandatory before this command and the protection mode of the RWM must be enabled.

### Command

The modes Addressed and Selected are possible.

Parameters required:

- Number of the page to be protected
- option flag must not be checked.

The figure below shows the detail and the meaning of the bytes sent from Controller to the RWM.

The Wireshark packet capture shows a packet from the Controller (FA) to the RWM (FE). The packet details are as follows:

- Start of frame : 0F
- Source : FA
- Destination : FE
- Packet length : 00 0D
- Sequence ID : 00
- Command number : 26 [Lock\_Page\_Protection]
  - Option : 20 (TAG addressed, option flag deactivated)
  - Mfg : 04 (Manufacturer code (NXP Semiconductors))
  - PgNum : 01 (Page number 1)
  - UID : E004020000568267 (TAG concerned)
- CRC : 05
- End of frame : F0

### Answer

The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.

The Wireshark packet capture shows a packet from the RWM (FE) to the Controller (FA). The packet details are as follows:

- Start of frame : 0F
- Source : FE
- Destination : FA
- Packet length : 00 03
- Sequence ID : 00
- Command number : 26 [Lock\_Page\_Protection]
  - Acknowledge : 00 (Operation successful)
- CRC : 6A
- End of frame : F0

## 27h Get Protection Status

### Effect of the command

Returns the protection state of the concerned blocks.

Block	Protection status [bin]
00	
01	
02	
03	00000000 00 - No password activated, page not locked
04	00001010 0A - Read password activated, page locked
05	00001010 0A - Read password activated, page locked
06	00001010 0A - Read password activated, page locked
07	00001010 0A - Read password activated, page locked
08	00000000 00 - No password activated, page not locked
09	00000000 00 - No password activated, page not locked
10	
11	

### Comment

Protection mode of the RWM must be enabled.

### Command

The modes Addressed and Selected are possible.

Parameters required:

- the address of the block from which the protection status will be carried out (Address block start)
- the number of blocks to examine (Number of blocks)
- option flag must not be checked.

The figure below shows the detail and the meaning of the bytes sent from Controller to the RWM.

```

28.01.10 15:33:01 : 0F FA FE 00 0E 00 27 20 04 03 06 67 82 56 00 00 02 04 E0 D0 F0
├── Start of frame : 0F
├── Source : FA Controller
├── Destination : FE RWM #254d
├── Packet length : 00 0E 14d
├── Sequence ID : 00
├── Command number : 27 [Get_Protection_Status]
│   ├── Option : 20 TAG selected, option flag deactivated
│   ├── Mfg : 04 Manufacturer code (NXP Semiconductors)
│   ├── BLStart : 03 3d
│   ├── NbBL : 06 6d
│   └── UID : E004020000568267 TAG concerned
├── CRC : D0
└── End of frame : F0
    
```

### Answer

The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.

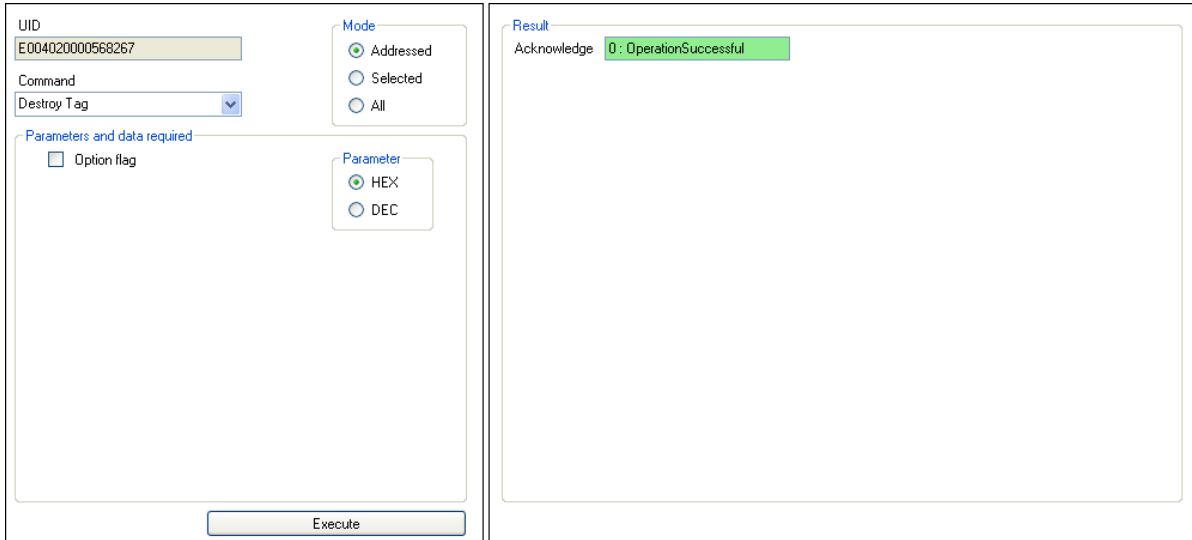
```

28.01.10 15:33:01 : 0F FE FA 00 0A 00 27 00 00 0A 0A 0A 00 00 D3 F0
├── Start of frame : 0F
├── Source : FE RWM #254d
├── Destination : FA Controller
├── Packet length : 00 0A 10d
├── Sequence ID : 00
├── Command number : 27 [Get_Protection_Status]
│   ├── Acknowledge : 00 Operation successful
│   └── Data : 00 0A 0A 0A 0A 00 00 Protection status for each block
├── CRC : D3
└── End of frame : F0
    
```

# 28h Destroy TAG

## Effect of the command

Deactivates, in an irreversible way, the transponder which will not answer any command any more.



## Comment

A login with Destroy TAG Password is mandatory before this command and the protection mode of the RWM must be enabled.

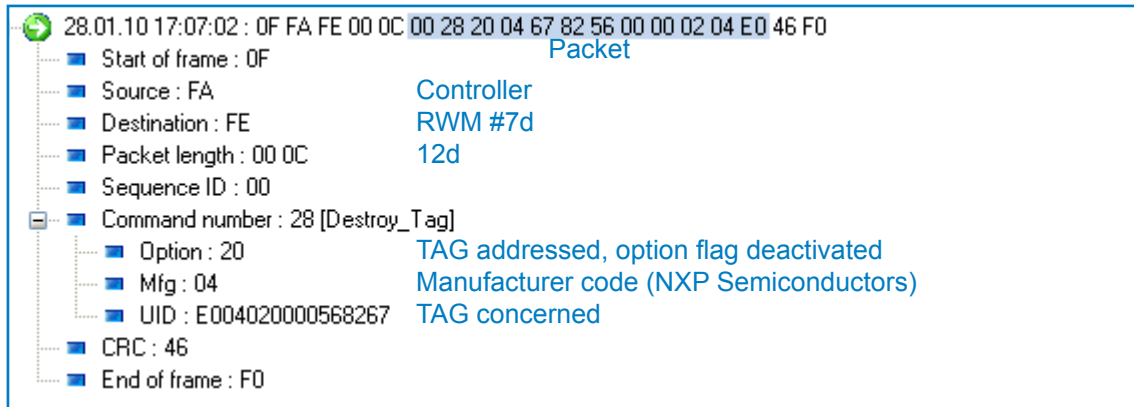
## Command

The modes Addressed and Selected are possible.

Parameters required:

- Number of the page to be protected
- option flag must not be checked.

The figure below shows the detail and the meaning of the bytes sent from Controller to the RWM.



## Answer

The figure below shows the detail and the meaning of the bytes sent from the RWM to the Controller.

