User manual
RFID IND Modbus-Mif

Soft >= v1.40

INVEO s.c.
ul. Rzemieślnicza 21
43-340 Kozy
Poland
mobile: +48 785 552 252
www.inveo.com.pl
info@inveo.com.pl

Dear Customer!

Thank you very much for choosing our product. Before its use, please read these instructions carefully. Here you find the most appropriate ways of dealing with this device, the basic principles of safety and maintenance. Please also keep the user manual so that you can read it during later use.

Remember!

The manufacturer is not liable for any damage caused by improper use of the device which differ from its intended purpose, or improper handling, as well as a fault of driver resulting from improper use.

Table of contents

1 Preliminary information

Before starting work with the device, read The User manual and follow the instructions contained therein!

Description of visual symbols used in this user manual:

This symbol is responsible for reviewing the appropriate place in the user instructions, warnings and important information. Failure to follow warnings could cause injury or damage to the reader

Important information and guidelines

Following this guidelines makes the use of the reader easier

Attention: The screenshots in this manual can be dissimilar from actual images at the time of the device purchase. Due to continuous development of the devices software, some of the functions may differ from these in the manual. The manufacturer claims no responsibility for any undesirable effects (misunderstanding) caused by changes of the software.

2 Applications of the device

The RFID IND Modbus-Mif device is used to read RFID Mifare Classic tags.
The device is used for an integration with other systems using Modbus RTU.

3 Warranty and liability of the manufacturer

The manufacturer provides a 2-year warranty on the device. The manufacturer also provides post-warranty service for 10 years from the date of the introducing the device on the market. The warranty covers all defects in material and workmanship.
The manufacturer undertakes to comply with the contract of guarantee, if the following conditions are met:

- all repairs, alterations, extensions and device calibrations are performed by the manufacturer or authorized service,
- supply network installation meets applicable standards in this regard,
- the device is operated in accordance with the recommendations outlined in this manual,
- the device is used as intended.

The manufacturer assumes no responsibility for consequences resulting from improper installation, improper use of the device, not following this manual and the repairs of the device by individuals without permission.

This device doesn’t contain serviceable parts.

4 Safety guidelines

The reader has been designed and built using modern electronic components, according to the latest trends in the global electronics. In particular, much emphasis was placed on ensuring optimum safety and reliability of control.
The device has a housing with a high-quality plastic.

4.1 Power supply

The module is suitable for power supply 10-24VDC.

4.2 Storage, work conditions.

The reader is equipped with a sealed IP65 enclosure which means:

- total resistance to foreign objects
- resistance to water jet directed directly to the device
- storage and operation at temperatures from -25°C to + 60°C,

4.3 Installation and use of the reader

The reader should be used following the guidelines shown in next part of the user manual.

4.4 Utilization of the reader

When it becomes necessary to liquidate the device (for instance retiring of the device from service), please contact the manufacturer or its representative, who are obliged to respond, appropriately, i.e. collecting the reader from the user. You can also ask the companies involved in utilization and/or liquidation of electrical or computer equipment. Under no circumstances should you place the device along with other waste material.

5 Construction of the module

5.1 General features

The reader is equipped with an RS485 port supporting Modbus RTU protocol and a USB port used for configuration and testing of the module.
The device has two relay outputs and two inputs.

Technical data:
Supply voltage:12-24VDC
Power supply: 40mA (12V)

Transponders:

Supported transponder standard: Mifare
Carrier frequency: 13,56 MHz
Reading distance to 10cm (depending on the type of transponder used)

Communication:

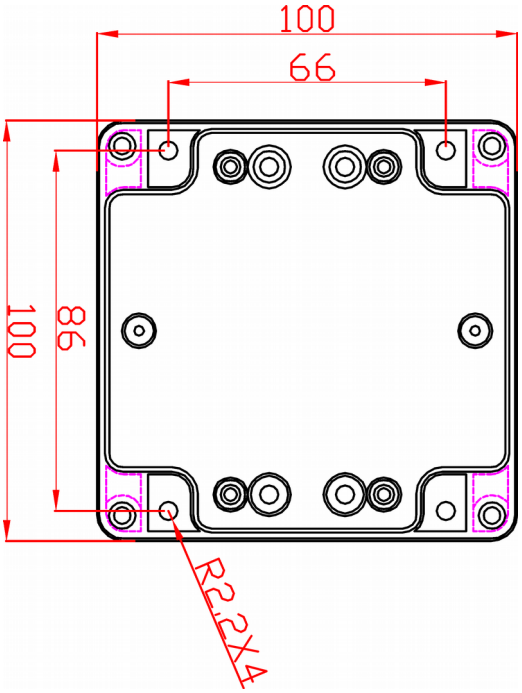
1 RS485 port – modbus RTU
1 USB port to configuration

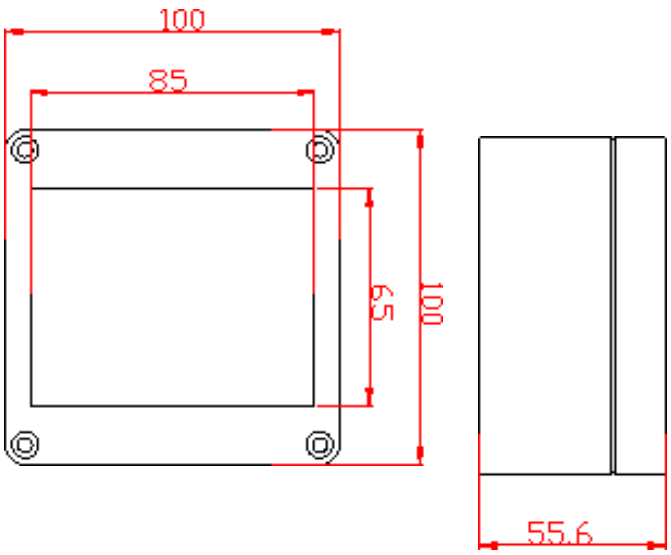
Inputs/Outputs

2 relay outputs 1A@30VDC
2 inputs

Enclosure:

IP Rating: IP65
Dimensions:





5.2 General view

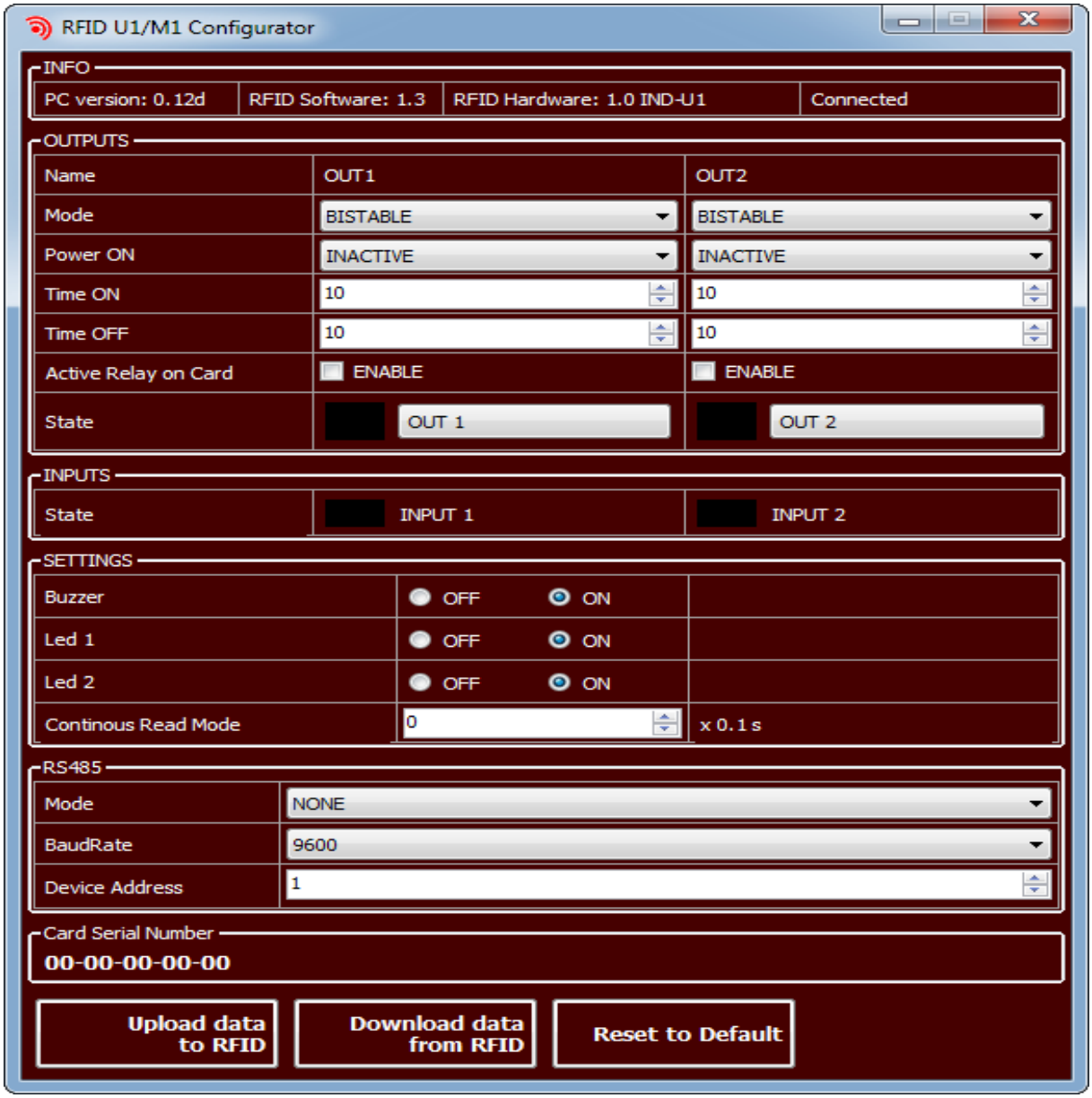
5.3 Visual and sound signals

The device has been equipped with 3 LEDs indicating the module operation status and a sound generator informing about the application of the tag.

RFID IND Modbus-Mif	
Name	**Description**
POWER	Power LED
Status 1	Error
Status 2	Correct tag read

6 Device configuration

To configure the device use the Inveo **RFID M1 / U1 Configurator** software, which allows you to define the basic functions of the device. The program can be downloaded from https://inveo.com.pl/software.
After installing the **RFID M1 / U1 Configurator** configuration program and starting it, connect the USB cable to the computer and the module (in this case, the external power supply of the module is not required – the device is powered via the USB port).



The first line of the program window displays information about the version of the configuration program – **PC version**, reader software version – **RFID Software** and reader version – **RFID Hardware**.

It is also an information on whether the configuration program was connected to a reader **Connected** / **Not connected.**

6.1 Outputs

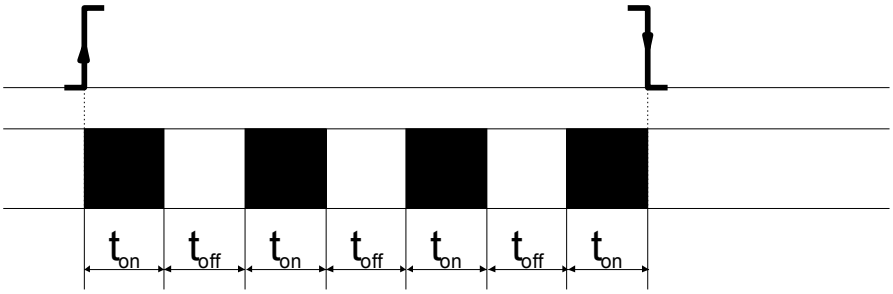
The reader is has 2 relay outputs. Each output can be programmed separately. The fields in the Outputs segment are used to configure the output settings.

Name	OUT1	OUT2
Mode	BISTABLE	BISTABLE
Power ON	INACTIVE	INACTIVE
Time ON	10	10
Time OFF	10	10

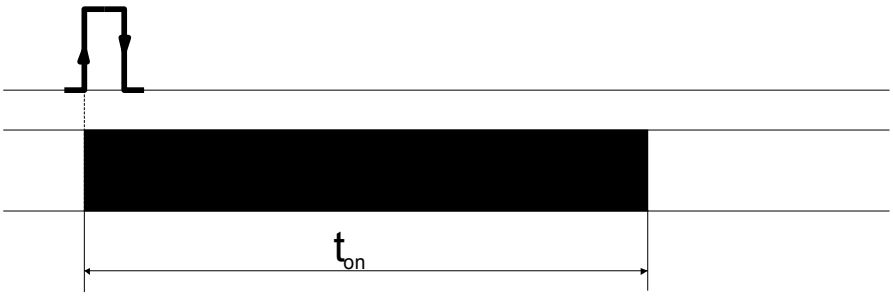
Mode – Sets the output mode. The output can work in the following modes:

- **Disable** – output is disabled,
- **Bistable mode –** a relay has one determined status (is engaged or disengaged).

- **Astable** mode – if the channel will be enabled, the relay is engage and disengage cyclically. Time of engage and disengage relay:
  - **Time On** – time when a relay is engaged,
  - **Time Off** – time when a relay is disengaged.



- **TIME** – the output will enable for the **Time ON** and then the output will disable (e.g. the control of the electromagnet).



Power ON – the state of the output after powering the device

- **Active –** output enabled,
- **Inactive** – output disabled.

State – visualization of the output, if a rectangle is yellow it means that the output current is turned on.
Buttons **Out 1** and **Out 2** outputs can activate or deactivate the output.

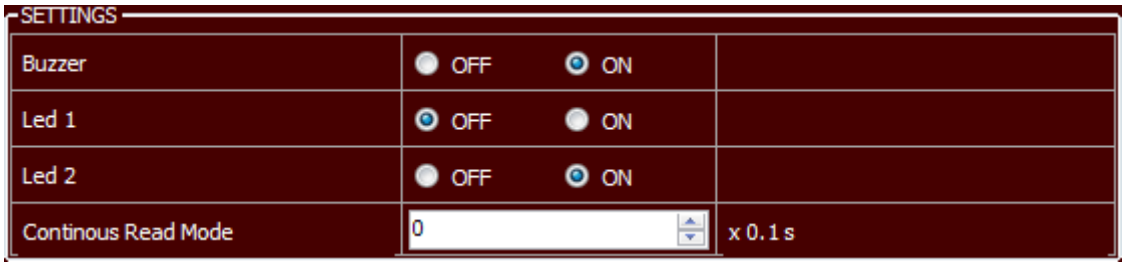
Active Relay on Card – if the TAG will be read, the output enables.
To set the duration of the active output it is necessary to select the **TIME** mode and set appropriate Time ON.

6.2 Inputs

Fields **STATE INPUT 1** and **STATE INPUT 2** displays the actual state of inputs. Square field in black – input inactive, field in yellow – active input.

6.3 LEDs and sound signaling control

The **RFID M1/U1 Configurator** allows user to customize visual and sound indication. All you have to do is select the appropriate configuration settings and upload it to the module.



Two options can be set for the Buzzer:

- OFF – signaling device switched off,
- ON – sound signaling at the moment of reading the TAG.

The device has 3 LEDs:

- Power supply diode, green LED,
- LED 1 – red LED,
- LED 2 – green LED.

Regardless of the selected setting, it is always possible to control the signaling via the Modbus RTU protocol.

6.4 Continuous Read Mode

The device allows the user to define the delay of reading TAGs.

The **Continuous Read Mode** means that the same TAG can be read only after the defined time has elapsed **but** another TAG is read immediately. This means that the same card will not be accidentally read several times. (30 = 3 seconds)

Attention! If the user uses this option, the read flag of the new TAG will **NOT** appear. The device will operate autonomously and automatically allow another reading of the same TAG after the declared time.

6.5 RS485 – Configuration of transmission

This field is used to configure the communication of the reader with the MASTER device.

MODE (setting of 9th bit of transmission):

- **None**
- **Even** – parity bit
- **Odd** – odd bit

BaudRate – transmission speed (**1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200**)
Device Address – device address for Modbus protocol

Card Serial Number – the field displays the last RFID transponder code read and the type of card.

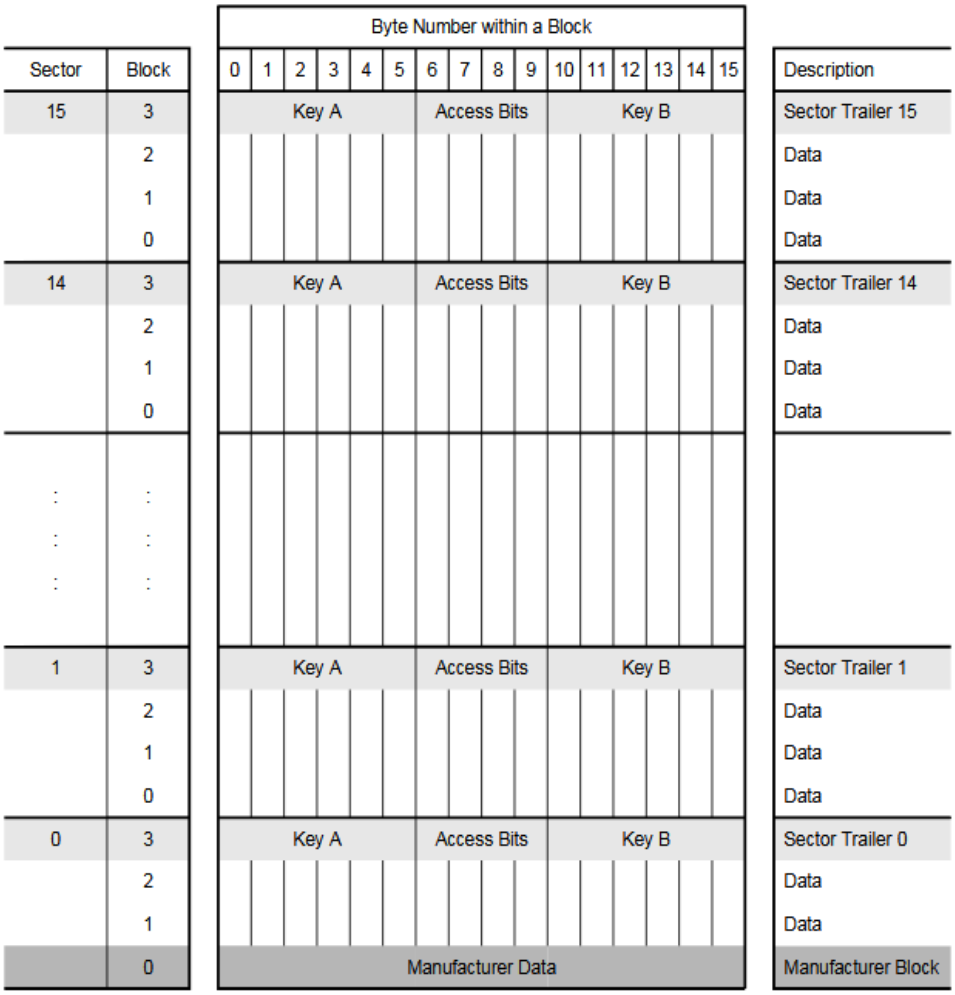
Attention! After customizing the settings and saving in the device, it is necessary to restart the device.

7 Modbus API

Modbus API allow user to:
- read and write any block of data from MIFARE tag
- set authorization credential for every Mifare tag blocks for write and read
- control user action (LED, Buzzer)
- control result of operation

7.1 Mifare tag structure

Below is Mifare 1k tag structure (note from NXP Semiconductor MF1S503x pdf):



Sector	Block	Byte Number within a Block 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	Description
15	3	Key A | Access Bits | Key B	Sector Trailer 15
	2		Data
	1		Data
	0		Data
14	3	Key A | Access Bits | Key B	Sector Trailer 14
	2		Data
	1		Data
	0		Data
:	:		
:	:		
:	:		
1	3	Key A | Access Bits | Key B	Sector Trailer 1
	2		Data
	1		Data
	0		Data
0	3	Key A | Access Bits | Key B	Sector Trailer 0
	2		Data
	1		Data
	0	Manufacturer Data	Manufacturer Block

Tag has 1kB EEPROM memory.
Memory is organized as 16-bytes block.
At one time tag can read or write exactly 16 bytes. So if user want to write 2 bytes to block without erase other, it is necessary to read 16 bytes, change 2 bytes and write 16 bytes.

Manufacturer Data
First block is Manufacturer Data. It is consist UID number (sometimes known as Card ID or Serial Number). In general it is readonly block but some manufacturer produce fake Mifare tag which be able to write that block.

Data block
Each sector contains 3 data blocks (except sector 0, which contains 2 blocks). Each block stores 16 bytes of data.
Data block can be configured by the access bit as:
- read/write block
- value block

Sector Tralier
At end of every block is Sector Trailer. It contains secret key:
- key A (obligatory key)
- key B (optionally key)
and configuration bits for access data block.

7.2 Modbus Address

The following MODBUS RTU functions are supported:
- 0x01 Read Coils
- 0x03 Read Holding Register
- 0x05 Write Single Coil
- 0x06 Write Single Register
- 0x0F Write Multiple Coils
- 0x10 Write Multiple Registers

⚠ **For proper operation of modbus protocol it is necessary to disable the RFID M1/ U1 Configurator application.**

Holding Registers table:

Address	R/W	Description
1000	R/W	**IsNewTag** 1-tag recognized 0-no tag **Flag must be reset (clear to 0) before read next tag.** Same as Coil Register 1016
1001	R	**UID Length** – lenght of Mifare UID (4,7 or 10)
1002 -1011	R	**UID**
1012	R	**Card Type**: type of read tag
1017	R	**MODEL ID**
1018	R	**Software Version**
1019	R	**Hardware Version**
1020	R/W	**Mode OUT1**: 1- bistable 2- astable 3- time
1021	R/W	**Time On OUT1** – time determining how long the output will be enabled (1-65535) (*0,1 sec) e.g. 120 = 12 seconds

Address	R/W	Description
1022	R/W	**Time Off OUT1** – time determining how long the output will be disabled (1-65535) (*0,1 sec)
1023	R/W	**Mode OUT2** output number 2 mode, as above
1024	R/W	**Time On OUT2** as above
1025	R/W	**Time Off OUT2** as above
2000	R/W	**WriteEnable** – Write TAG enable for next operation
2001	R/W	**ReadEnable** – Read TAG enable for next operation
2002	R/W	**TagType** – select 1k Mifare (0) or 4k Mifare (1)
2003	R/W	**MemoryMode** – linear (0) or full (1) buffer memory mode. See description
2004	R/W	**DataMode** – mode of representation data in buffer. (0-2) see description
2005	R/W	User Signaling mode for every recognized card: Format (binary): xxxx xxxx xxxx BB12 where: BB – 0 no signal, 1 signal accept, 2 signal reject 1 – led 1 2 – led 2
2006	R/W	User signaling mode for result read operation: Format (binary): xxxx xxxx EE34 BB12 where: EE – 0 no signal, 1 signal accept, 2 signal reject for error operation 1 – led 1 for error operation 2 – led 2 for error operation BB – 0 no signal, 1 signal accept, 2 signal reject for valid operation 1 – led 1 for valid operation 2 – led 2 for valid operation
2007	R/W	User signaling mode for result write operation Same as above.
2008	R/W	HaltTag – Write 1 will halt current tag and reader will be waiting for next tag. IsNewId and HaltTag is cleared after that.
2009	R/W	WakeAll – Write 1 release power from antenna for short time, so every Tag will be reset and accessible. IsNewId and WakeAll is cleared after that.
2010	R/W	ReadResultGlobal – result of last read operation: 0 no read error, 1 – error. It is logical sum of read errors at all readed block (ReadResultCode)
2011	R/W	ReadResultGlobal – result of last write operation: 0 no write error, 1 – error. It is logical sum of read errors at all written block (WriteResultCode)
2020-2035	R/W	RunReadFlag – select block for read operation. Each bit control one block. Ex. 0x0031 mean read block 0 from sector 0, and block 0+1 from sector 1
2040-2055	R/W	RunWriteFlag – select block for write operation. Each bit control one block.

Address	R/W	Description
2100-2355	R/W	ReadAuthorization – authorization setting for any block on read operation. Format (hex): xAxK, where: A – authorization type for block 0-A, 1-B, K-number of stored key 0-7. Ex. 0001 mean authorization type A and second stored key
2400-2655	R/W	WriteAuthorization – authorization setting for write operation. Same as above
2700-2955	R/W	ReadResultCode – result code for every read block operation (0-no error)
3000-3255	R/W	WriteResultCode – result code for every write block operation (0-no error)
4000-8095	R/W	Read Buffer Memory
10000-14095	R/W	Write Buffer Memory

Single Coil:

Address	R/W	Description
1000	R/W	**ON 1** – control relay 1 (off/on)
1001	R/W	**ON 2** – control relay 1 (off/on)
1002	R	**COIL STATE 1** – relay 1 coil state
1003	R	**COIL STATE 2** – relay 2 coil state
1010	R	**INPUT 1** – input 1 state
1011	R	**INPUT 2** – input 2 state
1012	R/W	**LED1** – control LED 1
1013	R/W	**LED2** – control LED 2
1014	W	**BUZZ ACCEPT** – enable accept sound
1015	W	**BUZZ REJECT** – enable reject sound
1016	R/W	**IsNewTag** 1-tag recognized 0-no tag **Flag must be reset (clear to 0) before read next tag.** Same as Holding Register 1000.
1017	R/W	**ResetFlag**: 1 – default state for power-on reader It can be clear and set by user for diagnostic purpose

In general use, you have to polling Coil 1016. When it change to 1 it is mean that the RFID device read new tag. Holding registers 1002-1011 contains tag ID.

When you read ID number you should release Coil 1016 (or Holding Reg 1000) flag (clear to 0). Only after that the reader is able to read next ID tag.

Modification of the output parameters can be done by the Modbus protocol. It is not stored in the module's permanent memory. That means after reboot, the output parameters previously saved to the EEPROM by the configuration program will be restored.

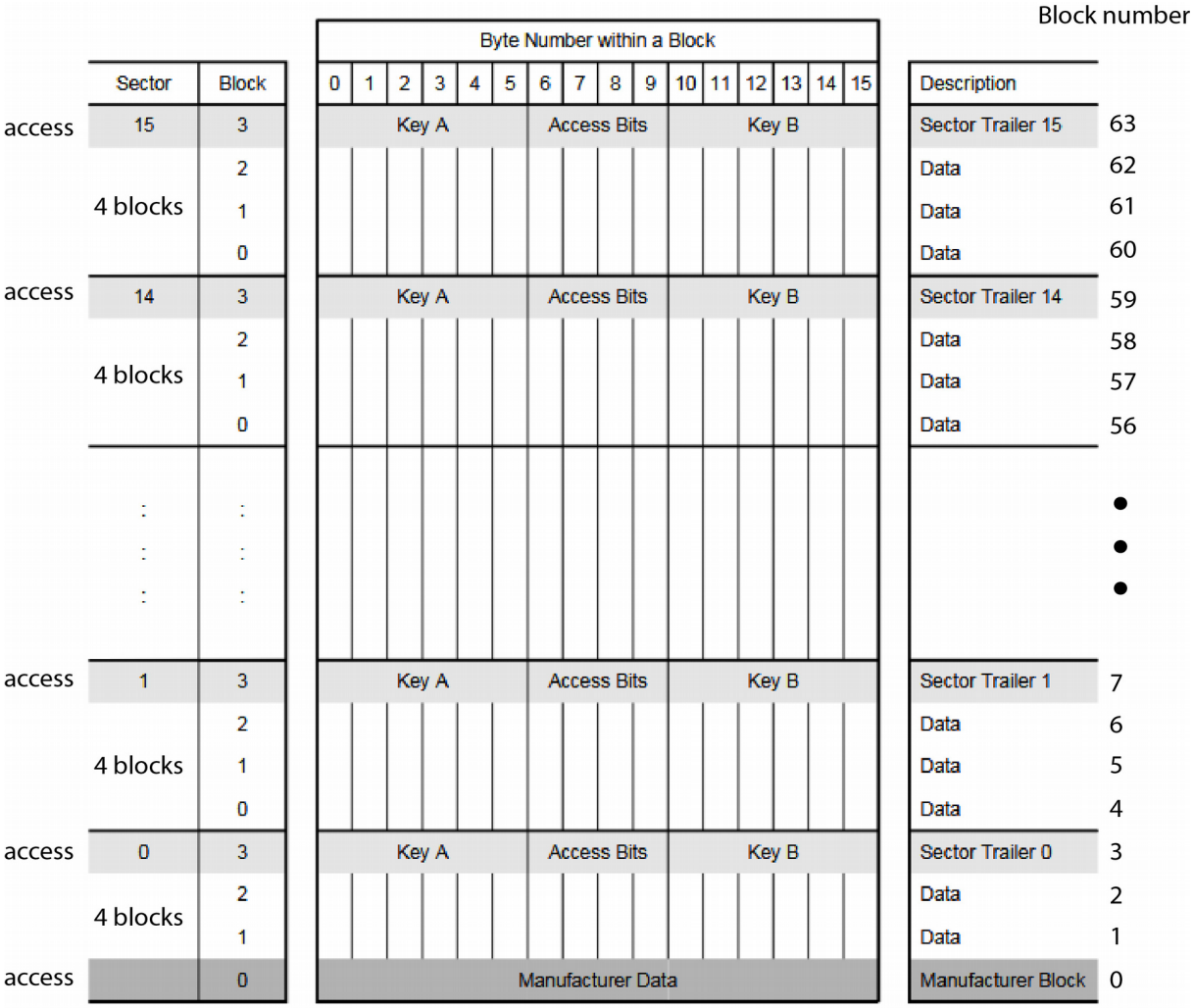
8 Memory buffer

RFID reader has built-in memory for store tag data. It is two 4kB buffers, first for read operation and second for write operation. Memory is accessible by Modbus Holding Registers.

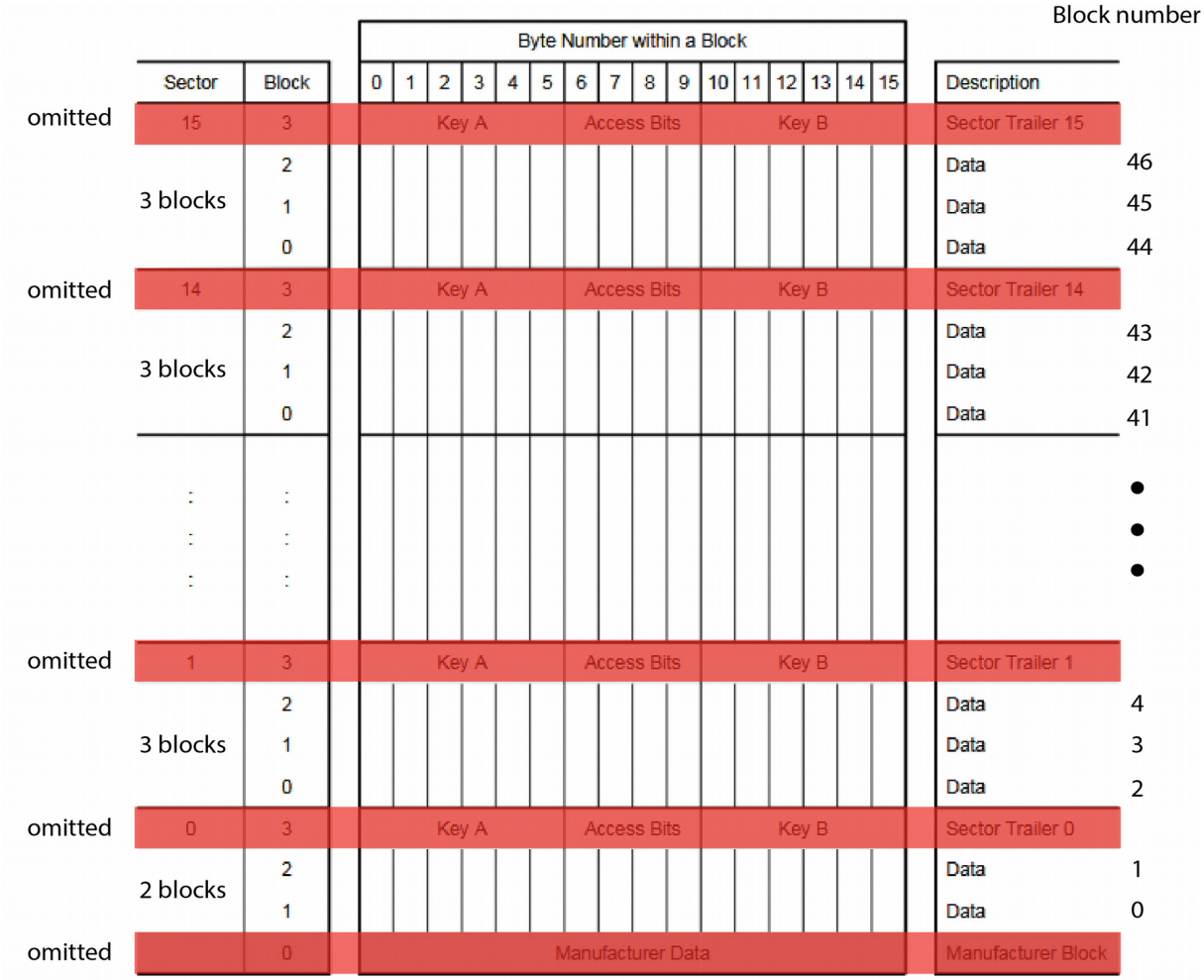
8.1 Memory buffer addressing

Reader can work at two types of memory adressing (reg MemoryMode)

- **Full mode** – read and write memory is addressed exactly like tag memory structure. To read second byte from fisrst block data user has to read 18 + buffer offset Modbus Register (1*16 + 2 = 18). Block 0 from 15 sector start at 15(sector number)*4(block in sector)*16(bytes in block) + offset Modbus Register. User must be careful to not write unwanted data to Sector Trailer because it can block access to sector.



- **Linear** – reader calculate address and omit manufacturer data and Sector Trailer block. User has 752 bytes for use at 1k Mifare tag. This mode is safe for Sector Trailer but application has not granted access to all tag data.



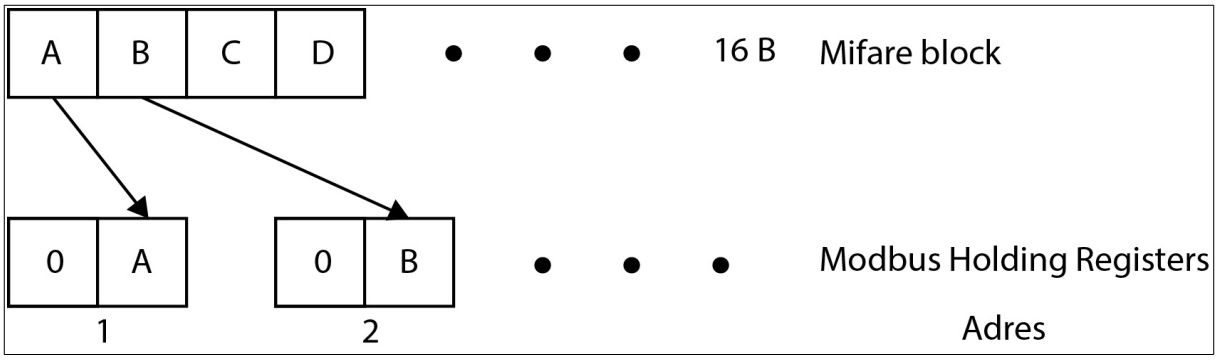
Attention!
RunReadFlag/RunWriteFlag has affect by this setting. When mode is **Linear**, RunReadFlag/RunWriteFlag omitt first block and any Trailer Sector. So first bit mean second block of first sector instead first block of first sector in **Full Mode**.

The memory addressing mode is set by sending the proper value: Linear mode (0) or Full mode (1) to the 2003 Holding Registers.

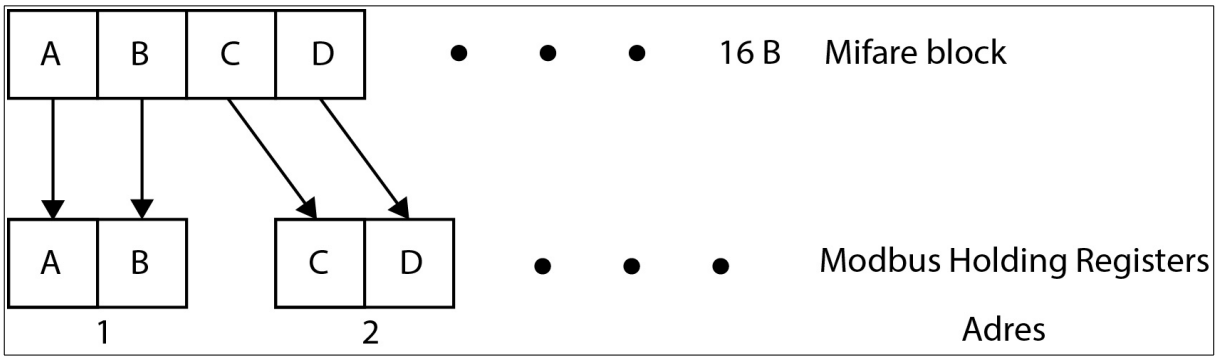
8.2 Buffer data representation (Endianess)

Reader has configuration for buffer data read/write modbus operation. There are 3 options (register DataMode):

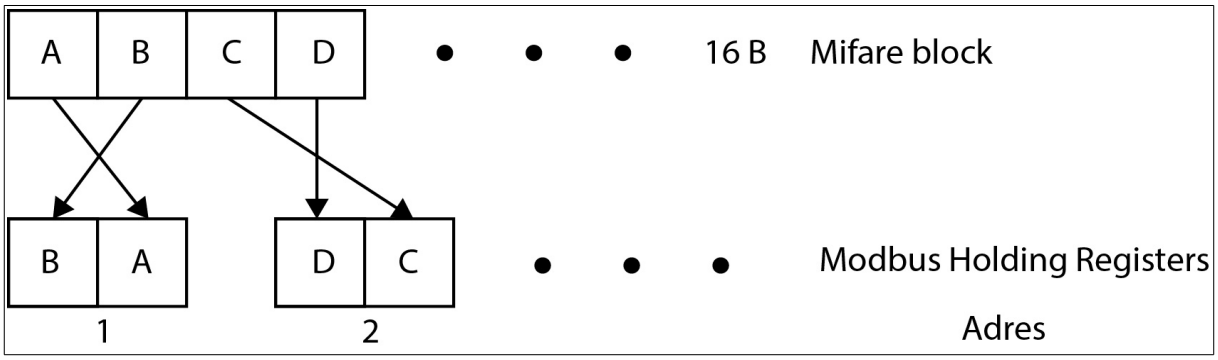
- **default** – every Modbus Holding Register keep one byte of tag data
  Example:
  If Tag block 0 has first two bytes: MSB:0x55 LSB:0xAA, than Modbus Reg 0(+Buffer Memory offset) contain 0xAA and Modbus Reg 1 constain 0x55



- **Endian 1** – every Modbus Holding Register contains 2 byte of data
  Example:
  If Tag block 0 has first two bytes: MSB:0x55 LSB:0xAA, than Modbus Reg 0(+Buffer Memory offset) contain 0x55AA



- **Endian 2** – every Modbus Holding Register contains 2 byte of data. *Example*:
  If Tag block 0 has first two bytes: MSB:0x55 LSB:0xAA, than Modbus Reg 0(+Buffer Memory offset) contain 0xAA55



Endian 1 and 2 can reduce data transfer between RFID Reader and Master Controller (PLC or other).

9 Block key

Followed by Mifare specification every block of data has own security setting. Trailer Sector descript which key (A or B) is needed to read and/or write block.

Key program is done by USB software. Factory security key for any block is key FFFFFFFFFFFF. Key is 6 bytes length. User can select one of 7 key stored in EEPROM write only memory. As default RFID Reader use FFFFFFFFFFFF key for all operation.

Every block has own selector of key and authentication type, separately for read and write operation (ReadAuthorization and WriteAuthorization registers).

10 Examples

10.1 Step by step Card ID read

1. Wait for 1 in IsNewTag register (1000 Holding Registers).
2. Read Card ID (1002-1005 Holding Registers).
3. Clear IsNewTag flag for enable reader.

10.2 Step by step read operation

1. Select User signaling mode (it can be omitted) for user response.
2. Select MemoryMode and DataMode.
3. If necessary set ReadAuthorization and WriteAuthorization for any block which has not default key and will be read.
4. Select block by set read flag bits (RunReadFlag) for block which has to be read.
5. Set ReadEnable flag (write 1).
6. Wait for 1 in IsNewTag register.

When tag is detected (IsNewTag=1) then:

7. Read selected memory area from ReadBuffer (4000-).
8. Do some signal to user for responce if not auto selected.
9. Optionally check ReadResultGlobal (2010) for error.
10. Clear IsNewTag flag for enable reader.
11. Go to step 6 for write another tag or do other things.

10.3 Step by step write operation

1. Select User signaling mode (it can be omitted) for user response.
2. Select MemoryMode and DataMode.
3. If necessary set WriteAuthorization for any block which has not default key and will be write
4. Write selected memory area by WriteBuffer (10000-). RunWriteFlags assigned for writing block is set automatic when write data to it.
4. Optional set or clear write flag (RunWriteFlag) for block which has to be write or not.
5. Set WriteEnable flag (write 1).
6. Wait for 1 in IsNewTag register.

When tag is detected (IsNewTag=1) then:

8. Do some signal to user for response if not auto selected
9. Optionally check WriteResultGlobal (2011) for error
10. Clear IsNewTag flag for enable reader
11. Go to step 6 for write another tag or do other things.

10.4 Step by step multiple tags

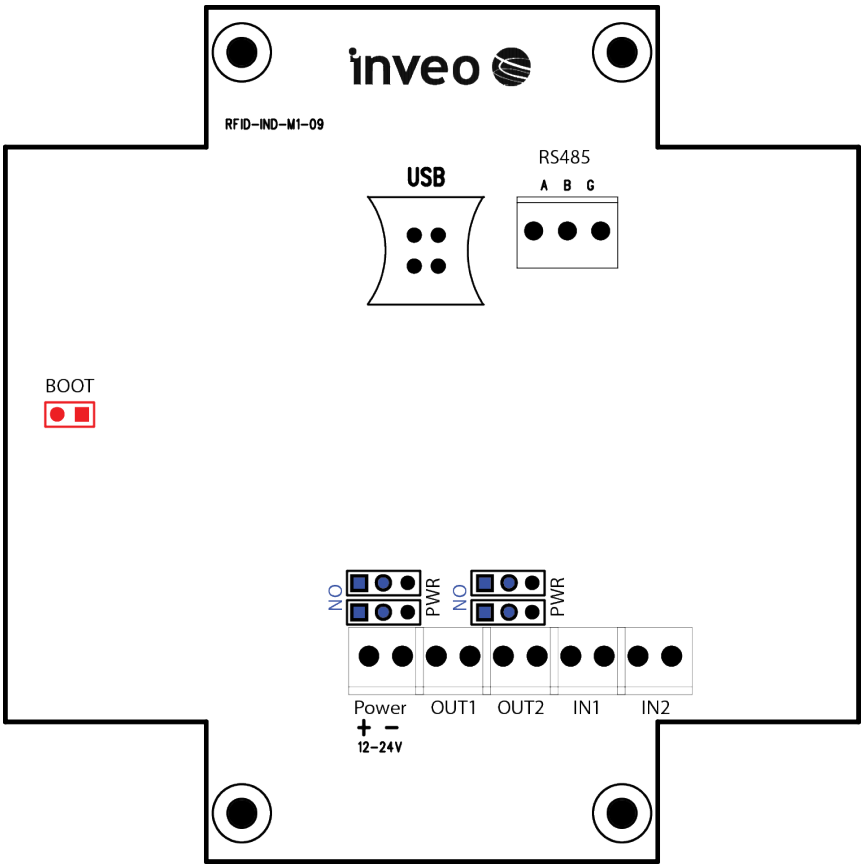
1. Wait for '1' in IsNewTag register.
2. Now do any operations (write, read, ...)
3. After all operation set 'HaltTag' to halt current tag and operate another

OR

4. Set WakeAll to reset all tags and operate again

11 Description of terminals

The view of the PCB is shown in the figure below.



Name	Description
Power	Power connector 12-24VDC
OUT 1	Relay output 1
OUT 2	Relay output 2
IN 1	Input 1
IN 2	Input 2
USB	USB port – module configuration
RS485	Connector RS485 MODBUS
Boot	Shortening the BOOT pins when power is applied causes the module to enter the bootloader mode