

RwProg



USER MANUAL

GENERAL INFORMATION	4
FEATURES	4
Additional items need to use this tool	5
TECHNICAL DATA	5
ACCESSORIES PROVIDED.....	5
THE GENERAL RECOMMENDATIONS	7
SOLUTION	8
HITAG2 TRANSPONDERS.....	9
Hitag2 reading procedure	10
Procedure for Configuring Hitag2	10
Procedure for Writing Hitag2.....	11
TEMIC ID11, ID12 TRANSPONDERS	12
Procedure for Reading Temic ID11, ID12	12
Procedure for Writing Temic ID11, ID12.....	13
MEGAMOS ID13 TRANSPONDERS	14
Procedure for Reading Megamos ID13	14
Procedure for Writing Megamos ID13.....	14
MEGAMOS CRYPTO ID48 TRANSPONDERS	15
TIRIS RO/RW ID4C TRANSPONDERS.....	17
Procedure for Reading Tiris RO/RW ID4C	17
Procedure for Writing Tiris RO/RW ID4C.....	17
TIRIS DST ID4D TRANSPONDERS	18
Procedure for Reading Tiris DST ID4D.....	19
Procedure for Writing Tiris DST ID4D	20
TIRIS DST+ ID4E TRANSPONDERS	21
TRANSPONDERS PIT (PCF7930/31/35/ELM).....	22
Procedure for Reading PIT (PCF7930/31/35/ELM)	22
Procedure for Writing PIT (PCF7930/31/35/ELM).....	23
CALCULATORS, COMPILER.....	25
FIRMWARE UPDATE.....	27

A decorative graphic consisting of a vertical blue line and a horizontal blue line intersecting at a point. The intersection area is shaded with a soft blue gradient, creating a crosshair effect.

INTRODUCTION

GENERAL INFORMATION

RwProg programmer has been designed to assist a locksmith specialists. **RwProg** is a duplicating device. Also this device can make transponders data from immobilizer units EEPROM file in case a customer has lost keys.

RwProg is able to read and display transponder memory electronic code and re-write it to a blank transponder. In case immobilizer EEPROM file is available, the device can also be used for restoration a lost keys by EEPROM data. The **RwProg** is device which ideally suited for repairing of the damaged transponders data.

- Identify transponder
- Read transponder codes
- Copy transponder
- Test transponder
- Generate fixed transponder codes
- Compiler for creation of programs-scripts by the user

FEATURES

RwProg show detailed information about transponders:

- transponder types
- transponder codes
- locked or not

RwProg can be used for reading, programming of low-frequency RFID transponders.

Table 1

№	Transponder type	Frequency	Operating		Note
			Read	Write	
1	Temic	125kHz	+	+	Copy to T5
2	Megamos	125kHz	+	+	Copy to T5
3	Megamos Crypto	125kHz	+	+	(*) Read UM1 and ID-code
4	Texas RO / RW	134.2kHz	+	+	Write to RW, copy to Keyline, 4C
5	Texas DST	134.2kHz	+	+	(*)
6	Texas DST+	134.2kHz	+	+	(*)
7	Phillips PIT (PCF7930/31/35/ELM)	125kHz	+	+	Read ID, identification IDE copy to PCF7935
8	Phillips Hitag-2	125kHz	+	+	(*)
9	Temic 8C	125kHz	+	-	(*)

(*) – unique serial number

Support of new transponder types can be added by program updating THROUGH THE OFFICIAL MANUFACTURER SITE!

Additional items need to use this tool

- 1) Host: x86 based PC, OS Windows 2000/XP/Win7
- 2) Free USB communication port.
- 3) Power supply: An stabilized DC 12 Volt / 500 mA

TECHNICAL DATA

MACHINE DIMENSIONS

Width: 220 mm
Height: 70 mm
Length: 150 mm
Weight: 0,4 kg

TECHNOLOGY FEATURES

Field frequency of transponder insertion slot: 125 kHz; 134,2kHz
Interface port: RS232 / USB (using USB-COM cable)
Working temperature 0°C to 40°C

ACCESSORIES PROVIDED

The device is supplied complete with:

- USB connecting cable
- Power jackplug
- Packing box



OPERATING WITH RWPROG

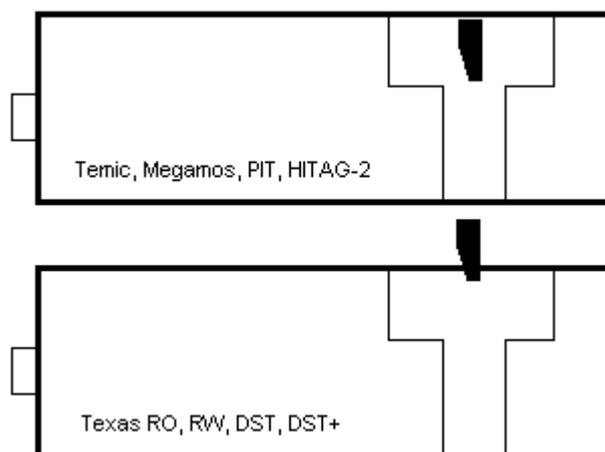
THE GENERAL RECOMMENDATIONS

USE ONLY TRANSFORMER BASED POWER SUPPLY!

The power voltage more than 12V is can damage device. Be careful and test twice power supply output voltage before connect to device!!!

If the software shows the message "The device not found", Select ⇒ Settings ⇒ tab Hardware. Select COM port to which the attached device. Close the program and run it again.

The best sensitivity for operations is indicated on the following picture. This condition is strongly recommended for Tiris transponders.



SOLUTION

1. Connect the device to computer, using the USB connecting cable.
2. Install USB drivers.
3. Connect the power supply (stabilized DC 12 volts 500mA) to device using the jackplug. (Jackplug is attached in pack). The contacts position - outside contact GND, inside contact +12V. Right connection is led indicated (the led is located near power connector).

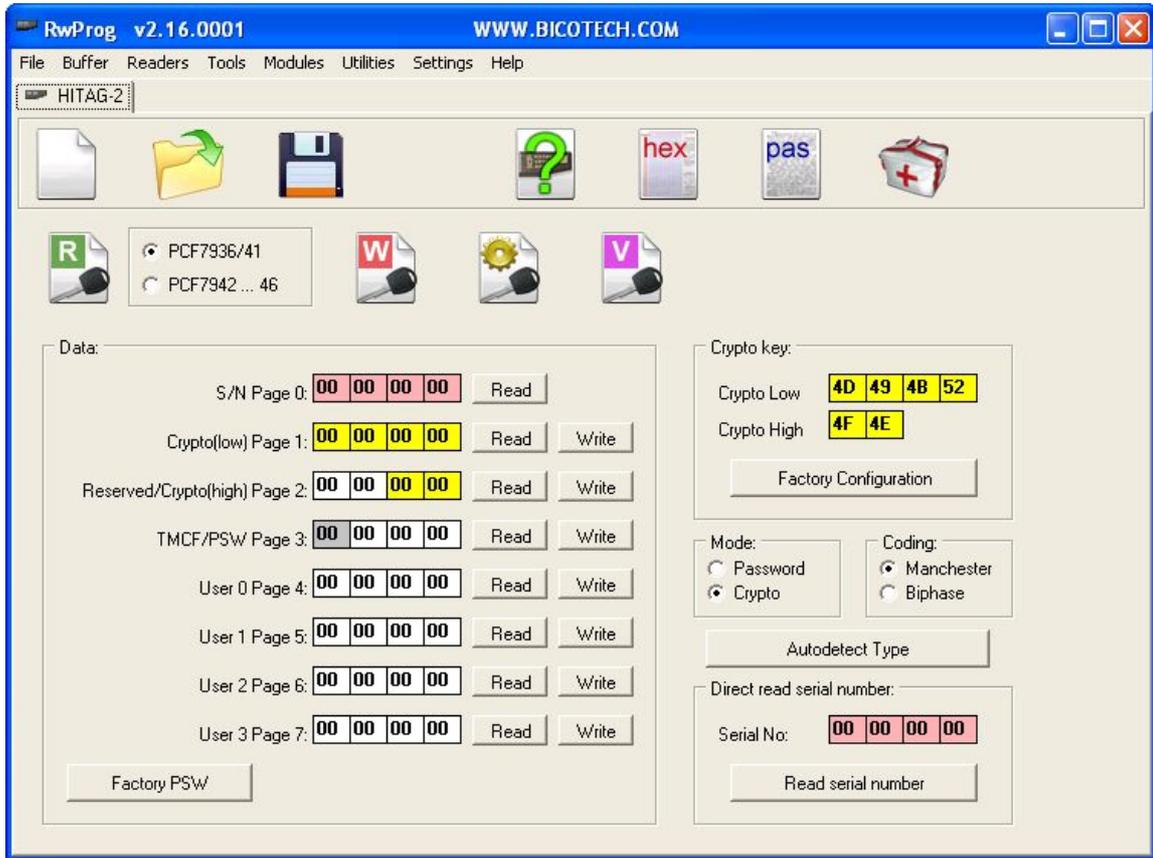
WARNING!!!!

The power voltage more than 12V is can damage device. Be careful and test twice power supply output voltage before connect to device!!!

4. Install the "RwProg" software.
5. The device is ready to work.

HITAG2 TRANSPONDERS

Open the software main window. Select ⇒ **Readers** ⇒ **HITAG2**



The tab is used for working with Philips transponders with HITAG2 crypto technology.

The memory of the transponder HITAG-2 consists of 256 bits EEPROM and is organized in 8 pages with 32 bits each. Depending on the mode of operation the EEPROM is organized in the following way:

crypto mode

Page No.	Content (32 bit words/ 4bytes)
0	ID number (serial number)
1	32 bit Key: "KEY LOW"
2	16 bit Key " KEY HIGH"
3	8 bit Configuration, 24 bit Password (Default = 06 AA 48 54 hex)
4	Read/Write page
5	Read/Write page
6	Read/Write page
7	Read/Write page

password mode

Page No.	Content (32 bit words/ 4 bytes)
0	ID number (serial number)
1	Password RWD (Default ="MIKR"=4D 49 4B 52hex)
2	Reserved
3	8 bit Configuration, 24 bit Password (Default = 06 AA 48 54 hex)
4	Read/Write page
5	Read/Write page
6	Read/Write page
7	Read/Write page

The software supports password mode of operation as well as crypto mode. Also you can choose data transfer mode: Biphase code or Manchester.

If You have new transponder, it is switched in transport mode. In this case mode of operation is "password", data transfer mode – Manchester code. On page opening

you will see initial password installed by manufacturer in top right corner of the window.

Please before programming of some transponder refer corresponding documents which describes features of transponder. Transponder must be programmed very carefully because some bits of transponder configuration can be programmed only once which leads to partial reading or programming of transponder.

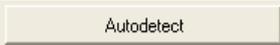
Hitag2 reading procedure

1. Select ⇒ **Readers** ⇒ **HITAG2**.
2. Insert transponder into the key reader (in centre of the coil on top side).
3. Click "**password mode**", if the transponder is set to password mode
Otherwise click to "**crypto mode**"

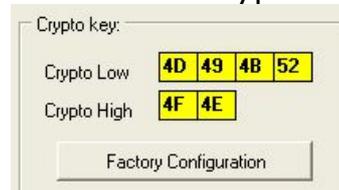


4. Click either Manchester or Biphase to select set data transfer mode

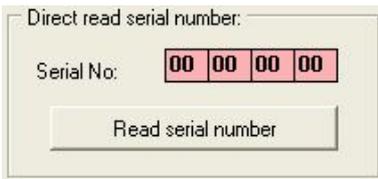


In case unknown mode or coding use  for an automatic detect data transfer mode.

5. Enter the password in the field either Crypto Low, Crypto High or Password



(depending on a mode)

6. Click  for direct reading of ID number (serial number)



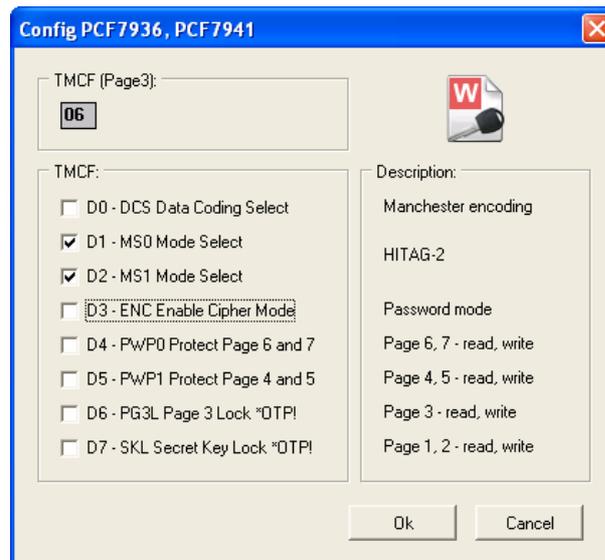
7. Click  for reading whole internal memory of transponder

Click "Read"  for reading separate pages only

Configuration data (Page 3 TMCf) is automatically translated in a bit mode and displayed in the TMCf field. This field is also editor of the configuration data.

Procedure for Configuring Hitag2

Click Config button



Change configuration bits using check boxes.

configuration bits using check boxes.

Click  .

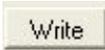


Or click  in case you want to program new configuration immediately.

Important! In chips with radio channel (PCF7942 ... PCF7946, etc.) bit configuration "D3 - USER page 4-7 visible" switch pages 4,5,6,7 from internal chip memory to remote memory bank.

Procedure for Writing Hitag2

1. Click  for writing whole internal memory of transponder

Click  for writing separate pages only

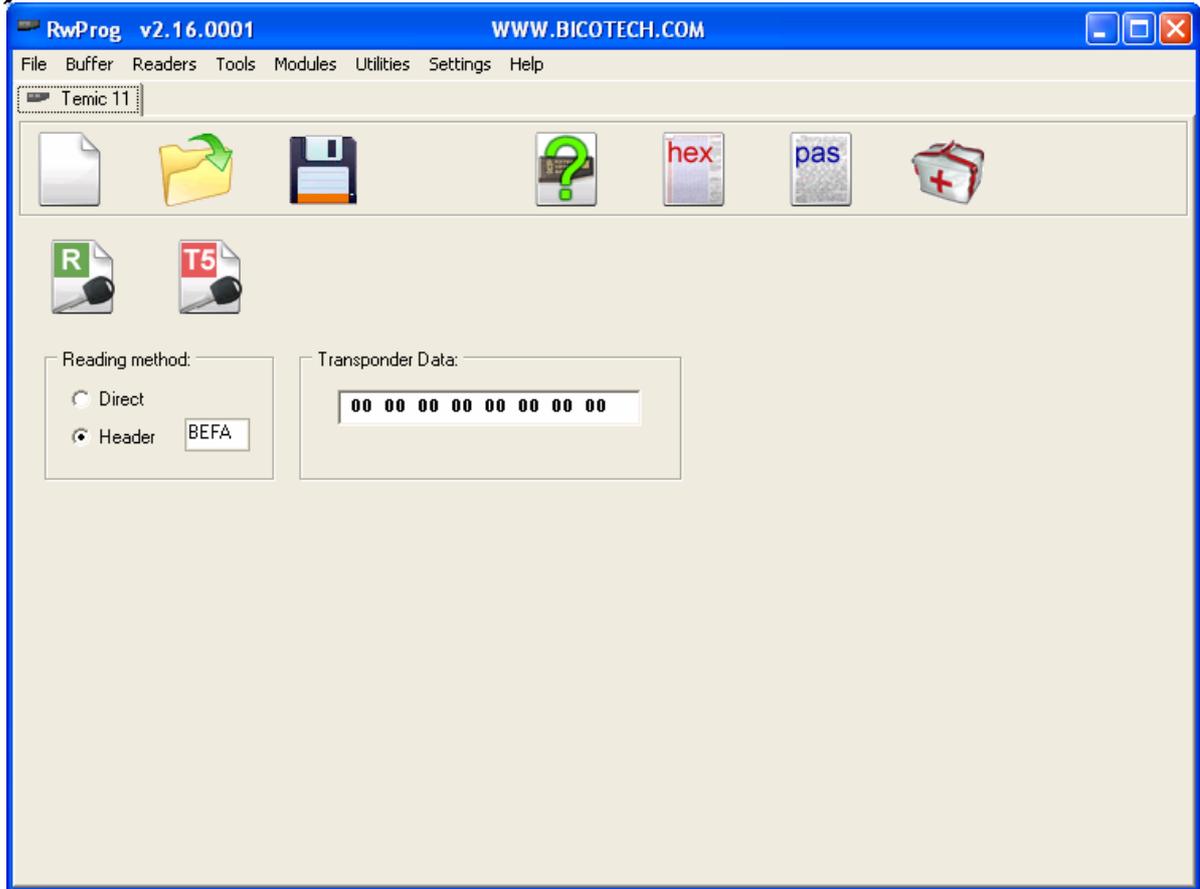
Note:

1. Page 0 is available for reading only, it contains unique transponder ID.
2. Do not forget to change password (crypto-key after writing Page 1 and 2 (that blocks contain password).
3. In case using separate pages writing, Page 2 must be writing at last (after writing of all other pages).

Click  for verify all.

TEMIC ID11, ID12 TRANSPONDERS

Open the main program window. Select ⇒ **Readers** ⇒ **Temic (11)** or **Temic (12)**



As transponder sends data cyclically in 16 bytes with NO block heading mark, you can't always get exact the same data as immobilizer of a vehicle does.

There are header bytes at the data. Point Header use for correctly reading the data. The software automatically will offer the correct title of the data for types ID11, ID12

Procedure for Reading Temic ID11, ID12

1. Insert transponder into the key reader (in centre of the coil on top side).
2. Click "**header**" and enter data, if the header data is known



Otherwise click to "**direct**"

3. Click  for reading internal memory of transponder

Note:

You can change, rewrite or save that data in binary format.

Procedure for Writing Temic ID11, ID12

1. Insert transponder into the key reader (in centre of the coil on top side).

Transponder Data:

00	00	00	00	00	00	00	00	00
----	----	----	----	----	----	----	----	----

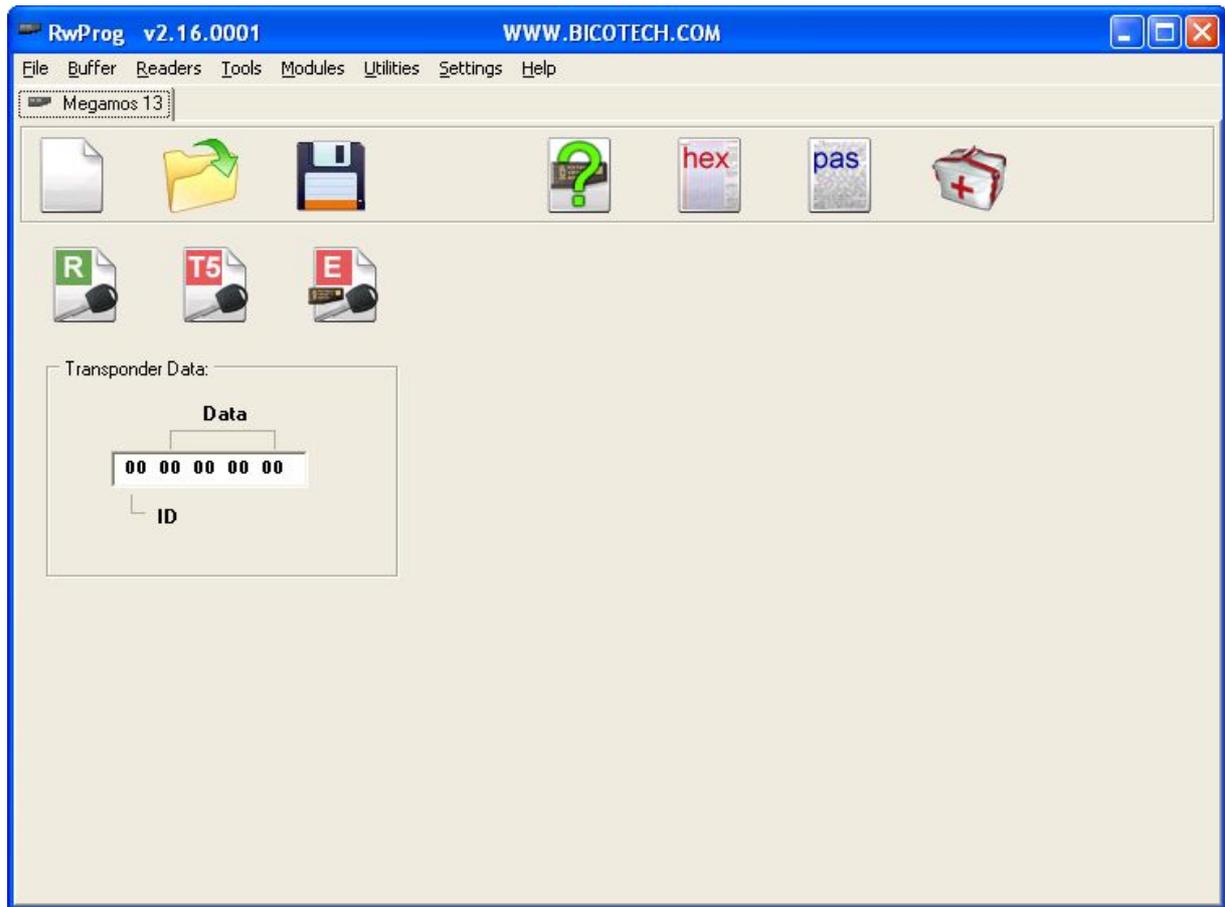
2. Enter data that you want to write



3. Click
4. Message will indicate in case writing was successful.

MEGAMOS ID13 TRANSPONDERS

Open the main program window. Select ⇒ **Readers** ⇒ **Megamos (13)**.



Operation with Megamos ID13 transponders is similar to operation with transponders Temic ID11, ID12 transponders. Difference is displayed data is corresponding to the real transponder data.

You can read, write transponder T5 or Philips PCF7935 in Megamos 13 emulation mode. Writing in a emulation mode becomes automatically.

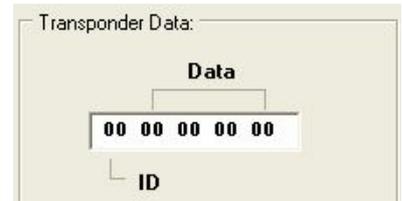
Procedure for Reading Megamos ID13

1. Insert transponder into the key reader (in centre of the coil on top side).

2. Click  for reading internal memory of transponder

Procedure for Writing Megamos ID13

1. Insert transponder into the key reader (in centre of the coil on top side).

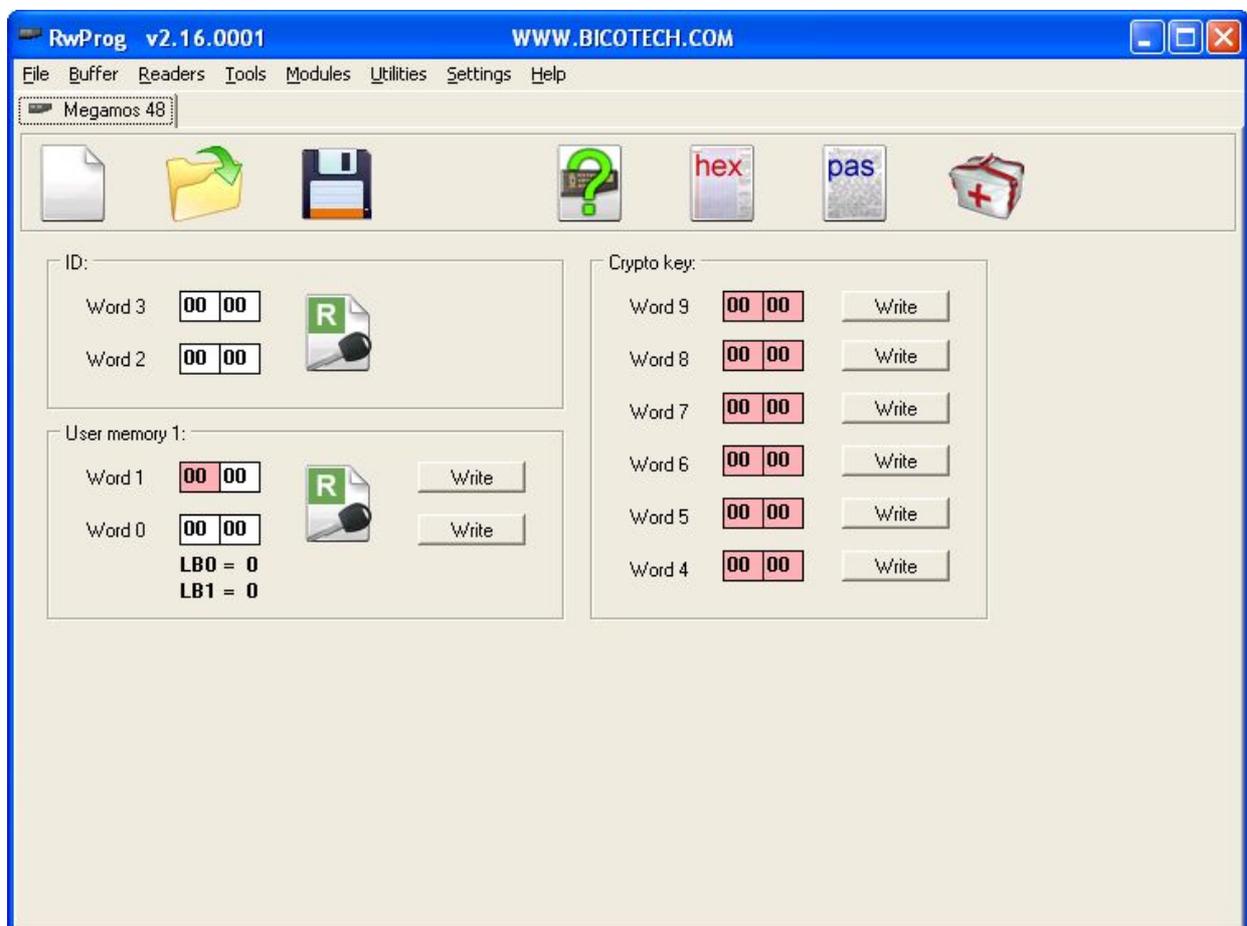


- Write down data that you want to write into the field or load data from file.
- Choose transponder type, in which the data should be written down: click

either  "T5" or  "PCF7935"

MEGAMOS CRYPTO ID48 TRANSPONDERS

Open the main program window. Select ⇒ Readers ⇒ tab Megamos Crypto (48).



Megamos Crypto ID48 is a high security Read-Write RFID Transponder. A challenge and response crypto algorithm with 96 bits of user-configurable secret key contained in EEPROM are implemented in the device.

The 160 bits EEPROM are organized in 10 words of 16 bits. Word 0 and 1 contain the USER-MEMORY and the LB1 and LB0 Lock-Bits.

Writing is only possible if LB1 = " 1" and LB0 = " 0" .

Words 2 and 3 contain the ID which can never be changed.

Words 4 ... 9 contain the 96 bits of secret-key. These bits influence the crypto-algorithm but cannot be read directly.

Procedure for Reading Megamos Crypto

1. Insert transponder into the key reader (in centre of the coil on a top side).



2. Click  and  and
3. Wait 100 % of read operation finished (the LED is stops flashing). The data from the transponder will be loaded in the editor.

Procedure for Writing Megamos Crypto

1. Insert transponder into the key reader (in centre of the coil on top side).
2. Type data that you want to write into the table or load data from file.
3. Choose the Words you want to write and Click . Wait 100 % of write operation finished (the LED is stops flashing).

TIRIS RO/RW ID4C TRANSPONDERS

Open the main program window. Select ⇒ Readers ⇒ tab Tiris RO/RW (4C) .



On the memory organization of TIRIS transponders are subdivided into some groups:
R/O (Read Only) Transponders – has the unique code , which doesn't change.
R/W (Read Write) Transponders - the user can read and change the code.

Procedure for Reading Tiris RO/RW ID4C

1. Insert transponder into the key reader (in centre of the coil on top side).



2. Click  for reading internal memory of transponder
3. Wait 100 % of end of read operation (the LED is stops flashing). The data from the transponder will be loaded in the editor. They become accessible to record in RW-transponder or emulators.

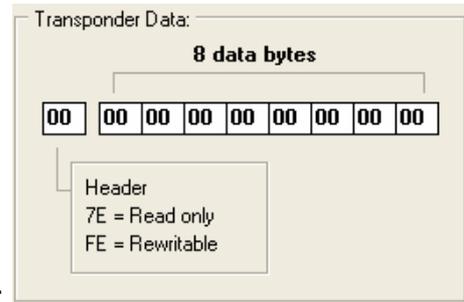
Procedure for Writing Tiris RO/RW ID4C

1. Insert transponder into the key reader (in centre of the coil on top side).

2. Type data that you want to write into editor load from file.



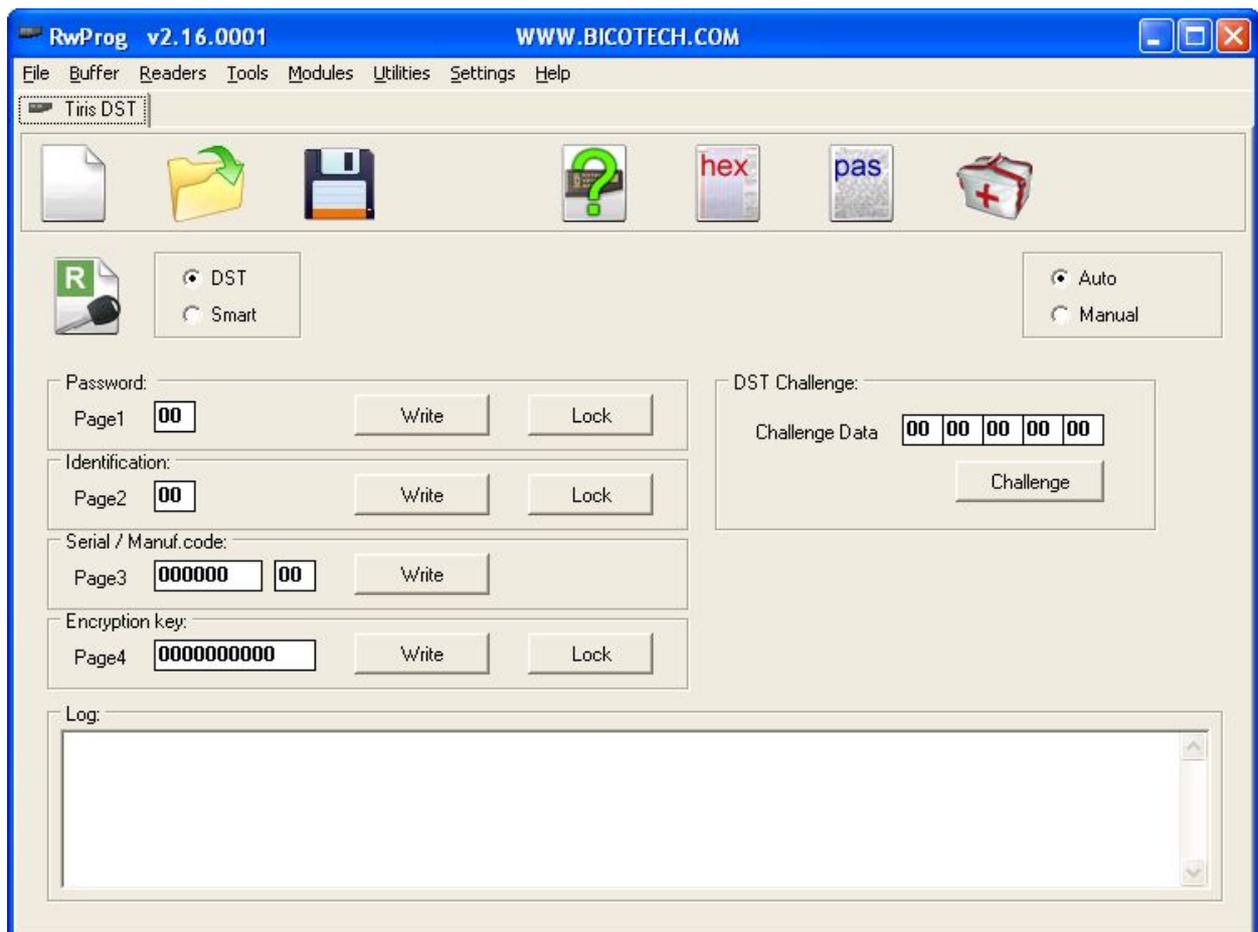
3. Click . Wait 100 % of write operation.



or

TIRIS DST ID4D TRANSPONDERS

Open the main program window. Select ⇒ **Readers** ⇒ **Tiris DST (4D)**.



The memory of the transponder Tiris DST ID4D is organized in 4 pages:

- Page 1 - Password;
- Page 2 - ID-code;
- Page 3 - Serial number / Manufacture code;
- Page 4 - Encryption Key.

Procedure for Reading Tiris DST ID4D

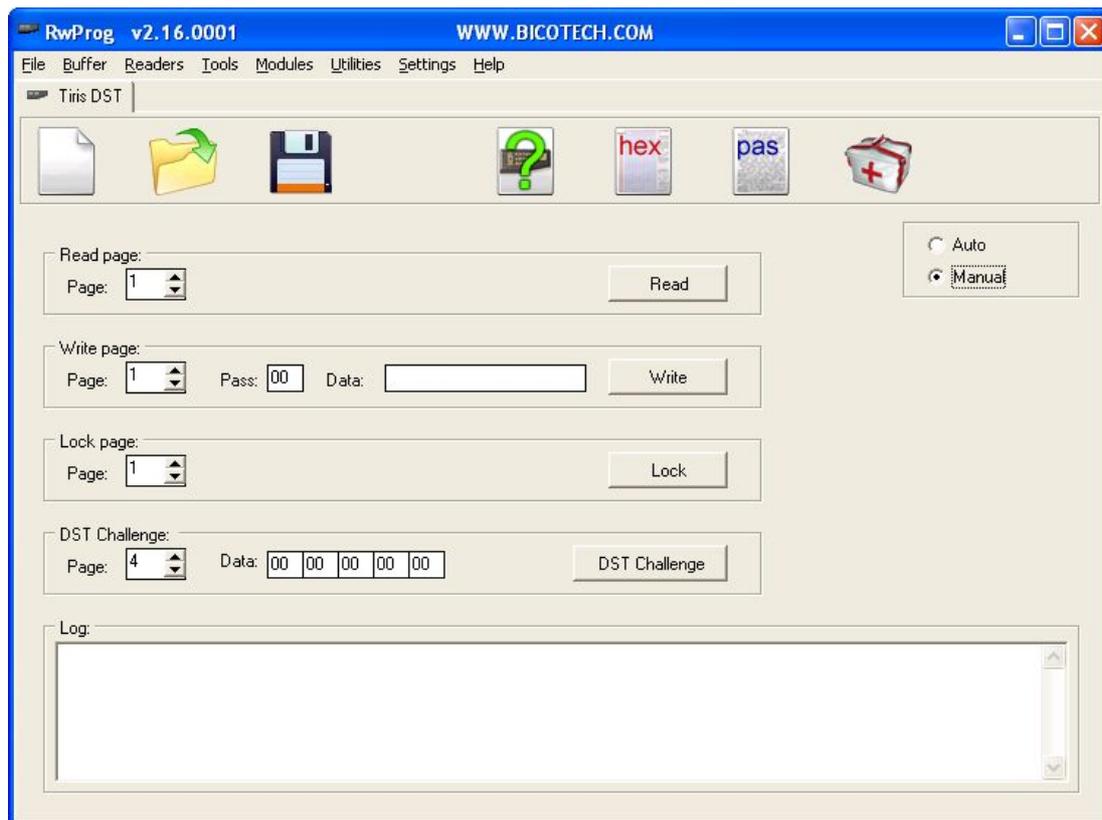
1. Insert transponder into the key reader (in centre of the coil on top side).
2. Choose transponder type: click either DST or SMART (with additional data



3. Choose transponder mode



4. Click  for reading in auto mode or 



in manual mode

5. Wait 100 % of read operation end (the LED is stops flashing). The data from the transponder will be loaded in the editor.

Note:

The Edited data indicated by green color

1. Enter data for DST Challenge

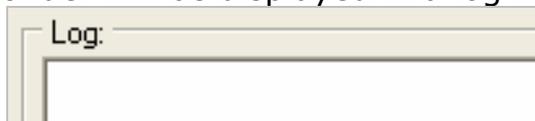
2. Click .

3. Data from the transponder will be displayed in a log field.



DST Challenge:

Challenge Data



Log:

Procedure for Writing Tiris DST ID4D

1. Insert transponder into the key reader (in centre of the coil on top side).

2. Write down data that you want to write into the editor or load data from file

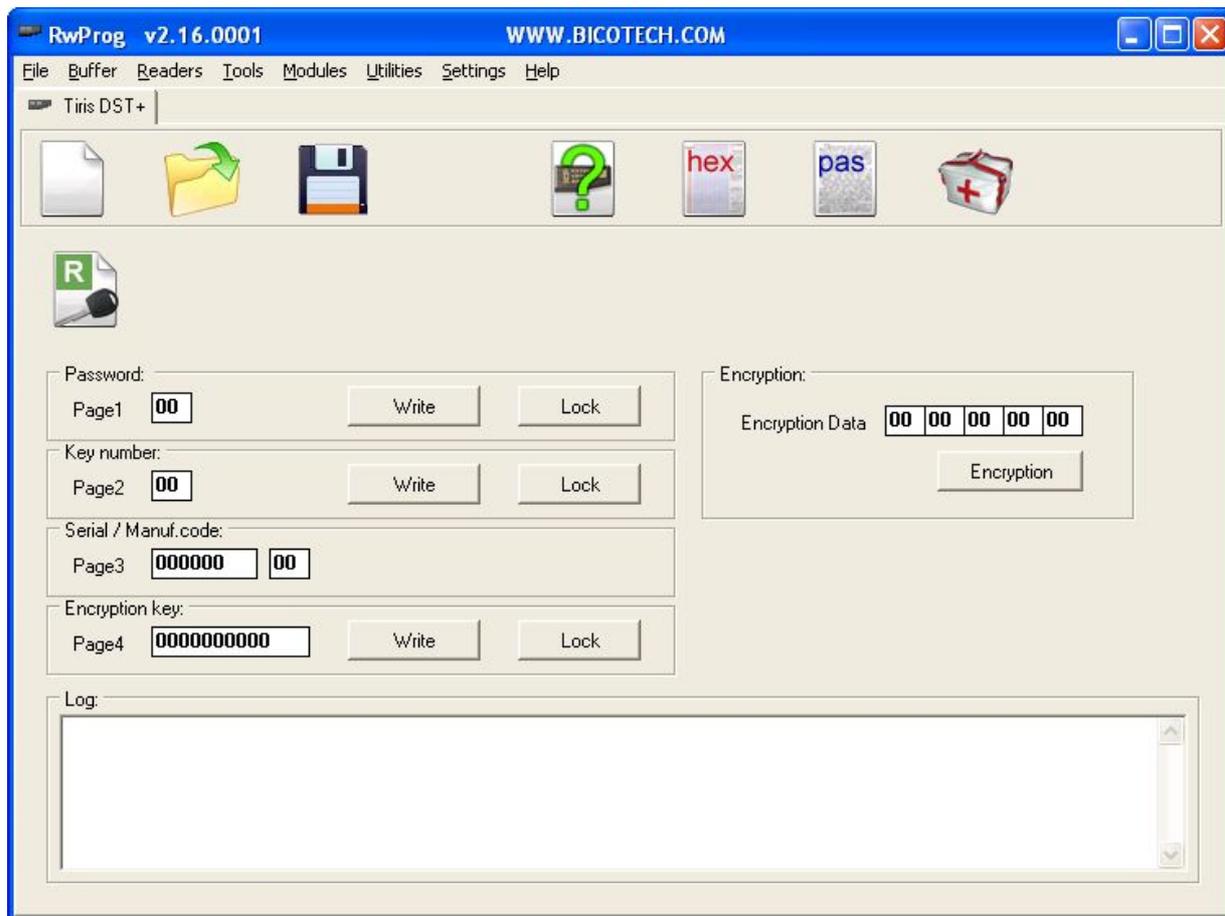
3. For writing separate pages only click 

4. For write protect data of Pages 1,2,4 click 

Warning! Operation of pages lock is irreversible.

TIRIS DST+ ID4E TRANSPONDERS

Open the main program window. Select ⇒ Readers ⇒ tab Texas DST +(4E)

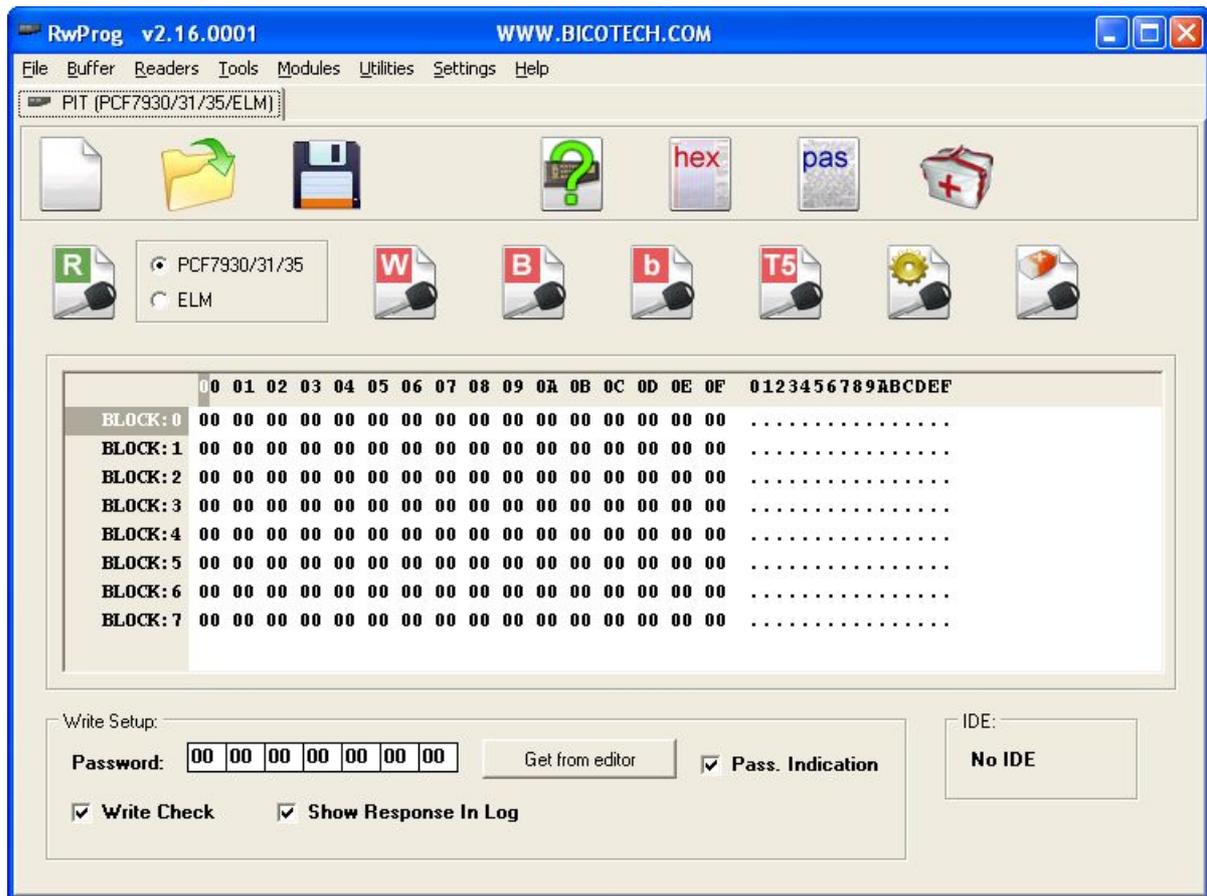


Operation with DST+ transponders is similar to operation with transponders DST transponders.

WARNING! DST+ transponder and DST transponder are not the interchangeable. They have differences in communication protocols.

TRANSPONDERS PIT (PCF7930/31/35/ELM)

Open the main program window. Select ⇒ **Readers** ⇒ **PIT (PCF7930/31/35/ELM)**.



The EEPROM are organized in 8 blocks of 16 bits:

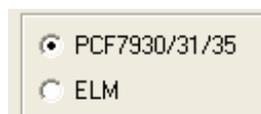
- Block 0,1 - Configuration memory
- Block 2...7 - user memory.
- PCF7935 has 1 more additional Shadow Block which can replace Block 2.

Such transponders have a lot of operation factors, so you have to be careful with recording blocks number 0 and 1, because of high risk of unrecoverable malfunction.

The tab has fields for different settings, and it is strongly recommended to read technical documentation of transponder before use.

Procedure for Reading PIT (PCF7930/31/35/ELM)

1. Insert transponder into the key reader (in centre of the coil on top side).
2. Choose transponder type: click either "PCF7930/31/35" or "ELM" (emulator of 7935 type in BMW vehicle electronic key).





3. Click  for reading transponder data. The data from the transponder will be loaded in the editor.

Note:

Warning! If The reading data consist less than from 8 units, then some part of the transponder is closed for reading.

If you see repeating lines in data table, it means that transponder is configured to send only some pages of internal memory. If you want to read all other pages, you need to write into block 1 two last bytes (RFB and RLB) data: 00 07 (that means blocks from 0 to 7 are open for read).

Warning!

Password is used only for transponder writing.

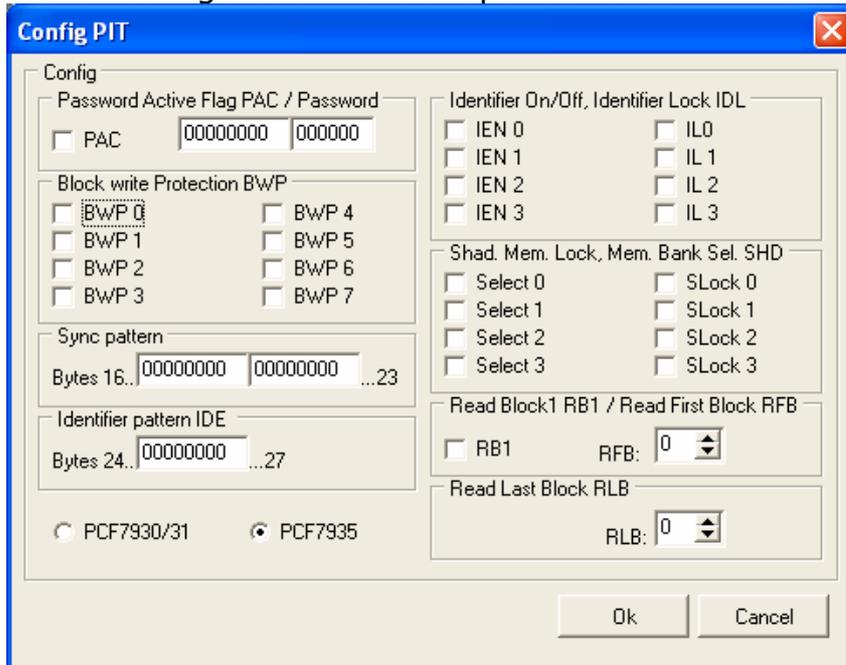
Transponder ELM has only 5 blocks. Blocks 0, 1, 2 is write only.

Procedure for Writing PIT (PCF7930/31/35/ELM)

1. Insert transponder into the key reader (in centre of the coil on top side).



2. Click  for a configuration of transponder data in window



Note:

If a password is activated on the transponder you can not write anything on it without known this password.

RFB and RLB bytes of configuration is setup blocks, which opened for the further reading.

Example:

RFB=2, RLB = 7. In this case blocks 2 - 7 will be open for reading. After program the reading data don't contain blocks 0 and 1.



3. Click

PIT transponders support 2 write modes – block mode and byte mode.

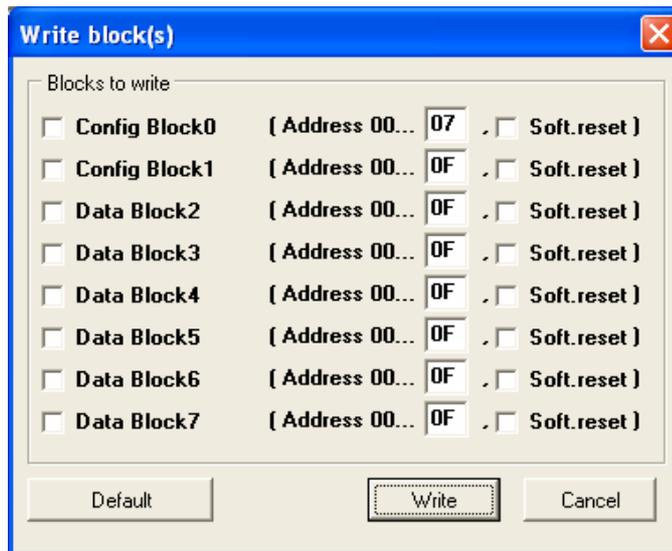


Click

Warning!

Transponders ELM support only a mode of byte-serial writing.

Change block 0 data of ELM transponder, excluding the password (addresses in the block 07 ... 0Fh) is lock the transponder.



You can choose block and byte addresses in this block what you want to write, or

leave without changes. Click



For write in a manual mode following steps are recommended:

Write in byte-mode RFB = 00h, RLB = 07h.

Write all transponder data, except bytes RFB, RLB. At record in the block 1 specify addresses of write 00 ... 0D.

Read data transponder. Compare the reading and writing buffer. In case of need, repeat write.

Change RFB, RLB, using a Byte-mode writing.

T5 transponder has possibility to emulate Philips PIT transponder, so You can

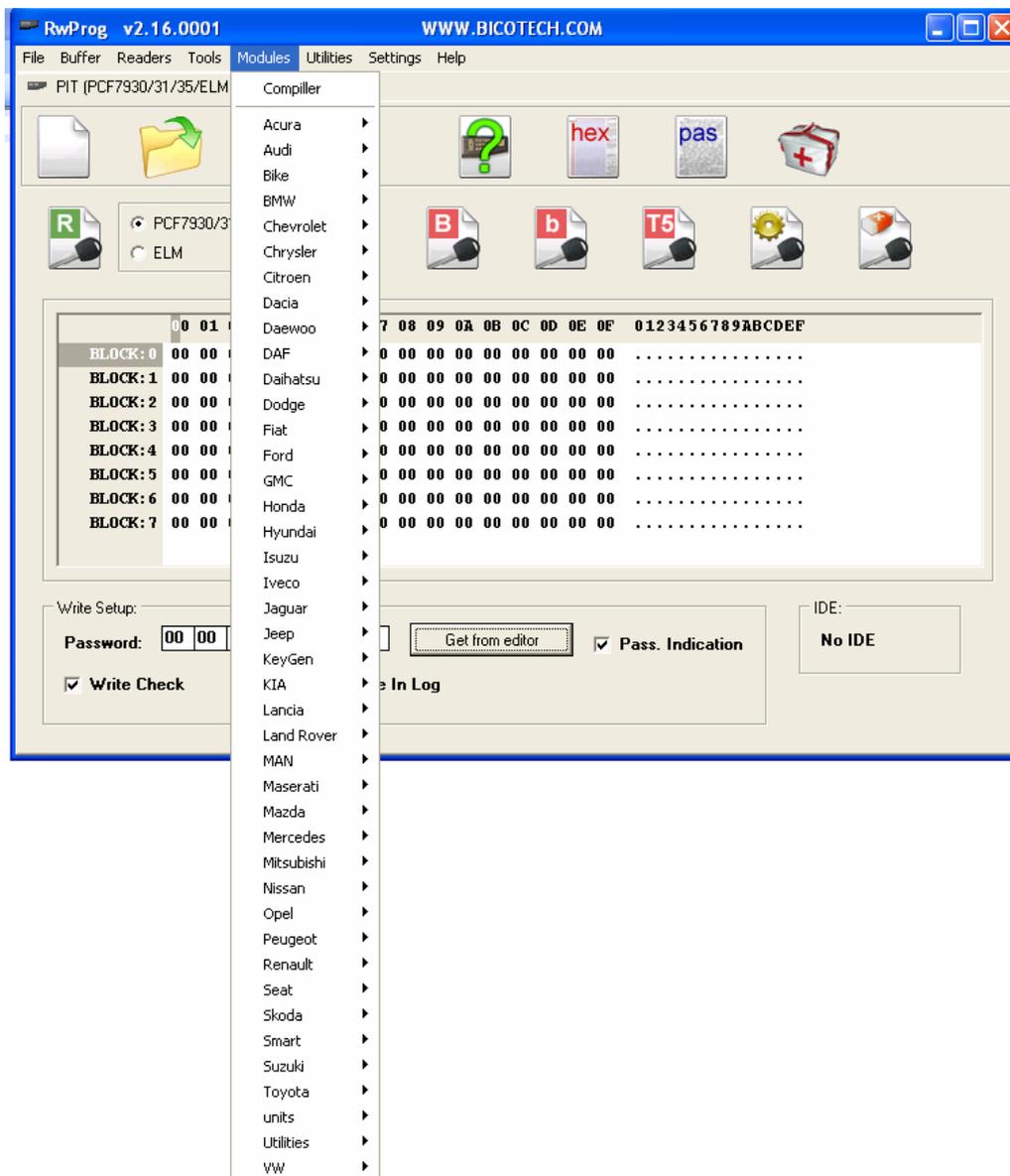
write any one block data on it in "Philips emulation mode"



CALCULATORS, COMPILER

There are set of calculators in RwProg software menu that allow to compute data needed for transponder writing based on immobilizer EEPROM memory dump.

Also by means of RwProg software menu it is possible to use on-line calculators. Function is intended that Users could work with the latest versions of calculators. The list of calculators is permanently updated.



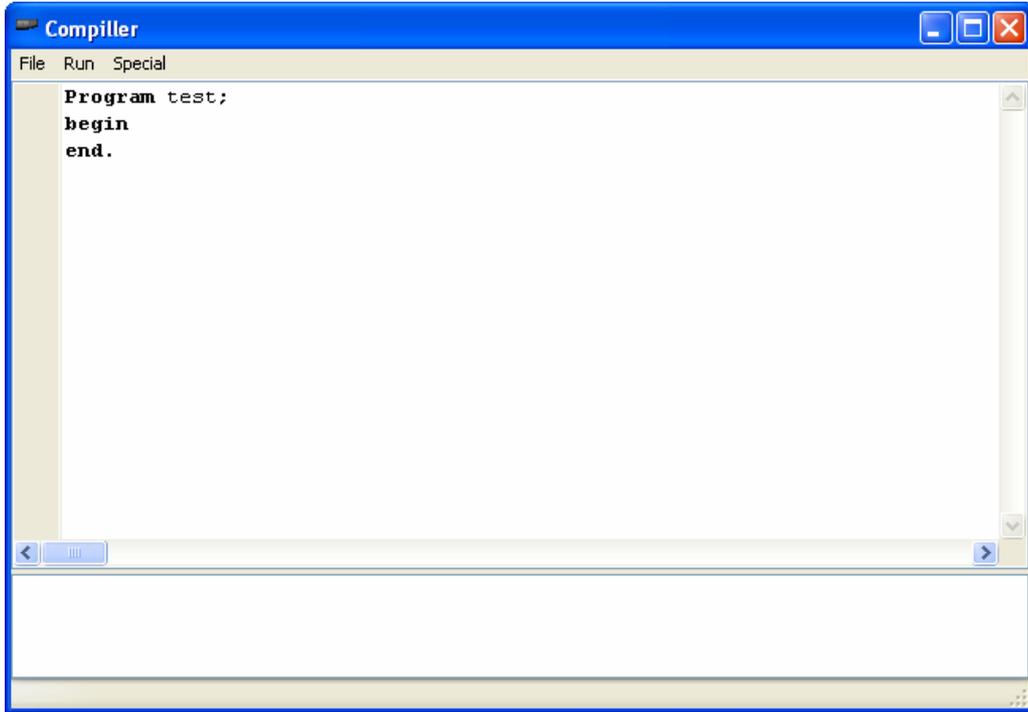
Device RwProg has additional engineering functions for professionals that allows to use its possibilities much more widely.

The compiler of scripts allows the user with minimum knowledge of Pascal language independently to create programs-scripts for automation of any process.



Click

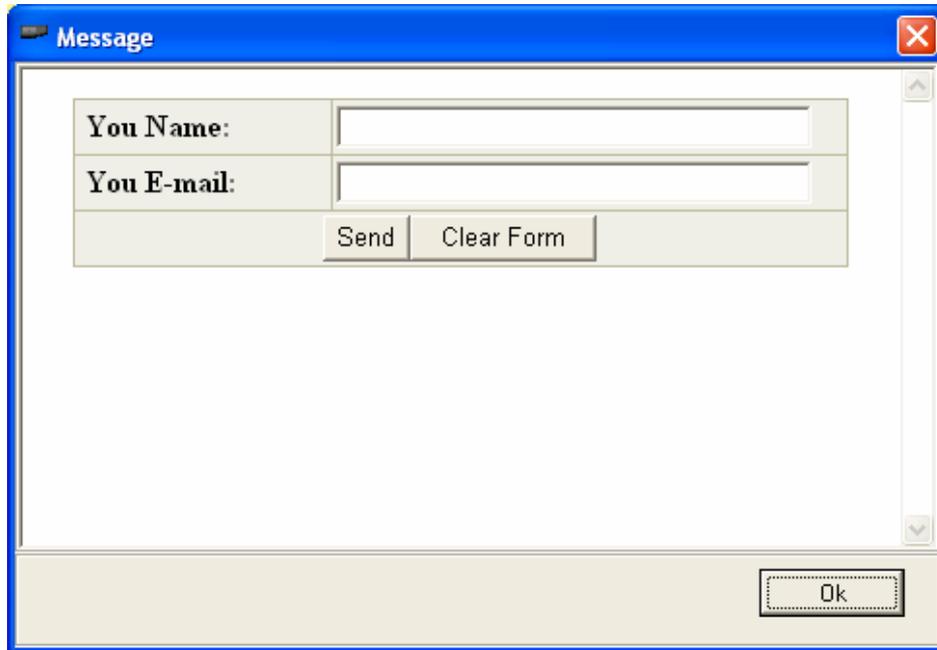
Example: creation of the transponder data on the basis of the data from a file.



FIRMWARE UPDATE

Support of new transponder types can be added by firmware updating THROUGH THE OFFICIAL SITE OF THE MANUFACTURER!

Select ⇒ **Utilities** ⇒ **Update request** for send request.



The image shows a Windows-style dialog box titled "Message". It contains two text input fields: "You Name:" and "You E-mail:". Below these fields are two buttons: "Send" and "Clear Form". At the bottom right of the dialog box is an "Ok" button. The dialog box has a blue title bar and a standard Windows window border.