USER MANUAL

HT EV801

HITAG™ Long Range Evaluation Kit

Preliminary Product Description
Revision 1.00

October 2005

Frosch Electronics OEG

hitag™

- is the name of one of the universal and powerful product lines of the 125 kHz family. The HITAG product family is used both in the proximity area (reading range up to about 300 mm) and in the long range area (reading range up to 2 m).

Developing our HITAG products, utmost consideration was given to security and reliability. The use of cryptography guarantees highest data security.

Using optimized antennas and powerful transponders operating ranges of up to 2 m can be achieved.

The central part of every HITAG Read/Write Device is the HITAG Core Module, which ensures full compatibility for every HITAG Read/Write Device.

Easy integration and application of the HITAG Core Module is due to its:

- small size
- standard interfaces
- flexible supply voltage

To give you the possibility for an easy and quick start with our HITAG products we offer a HITAG Long Range Evaluation Kit.
Easy application certainly is an important factor in making the Long Range Evaluation Kit suitable for evaluation purposes. You will be able to present your ideas and demonstrate the performance of your system with the help of the HITAG Evaluation Kit.

hitag™ Long Range Evaluation Kit Description

TABLE OF CONTENTS

Definitions

Data sheet status	
Objective specification	This data sheet contains target or goal specifications for product development.
Preliminary specification	This data sheet contains preliminary data; supplementary data may be published later.
Product specification	This data sheet contains final product specifications.
Limiting values	
Limiting values given are in accordance with the Absolute Maximum Rating System (IEC 134). Stress above one or more of the limiting values may cause permanent damage to the device. These are stress ratings only and operation of the device at these or at any other conditions above those given in the Characteristics section of the specification is not implied. Exposure to limiting values for extended periods may affect device reliability.	
Application information	
Where application information is given, it is advisory and does not form part of the specification.	

Life support applications

These products are not designed for use in life support appliances, devices, or systems where malfunction of these products can reasonably be expected to result in personal injury. Customers using or selling these products for use in such applications do so on their own risk and agree to fully indemnify Philips for any damages resulting from such improper use or sale.

1. General Remarks

1.1. Scope of Delivery

The Proximity Evaluation Kit comprises the following components:

- 1 HITAG proximity read/write device
- 1 Interface cable
- 1 Power supply
- 1 CD-Rom with evaluation software, data sheets and product information
- Transponders

The Long Range Evaluation Kit comprises the following components:

- 1 HITAG Long Range read/write device
- 1 Flat cable antenna (optional PCB antenna)
- 1 Interface cable
- 1 Power supply
- 1 CD-Rom with evaluation software, data sheets and product information
- Transponders

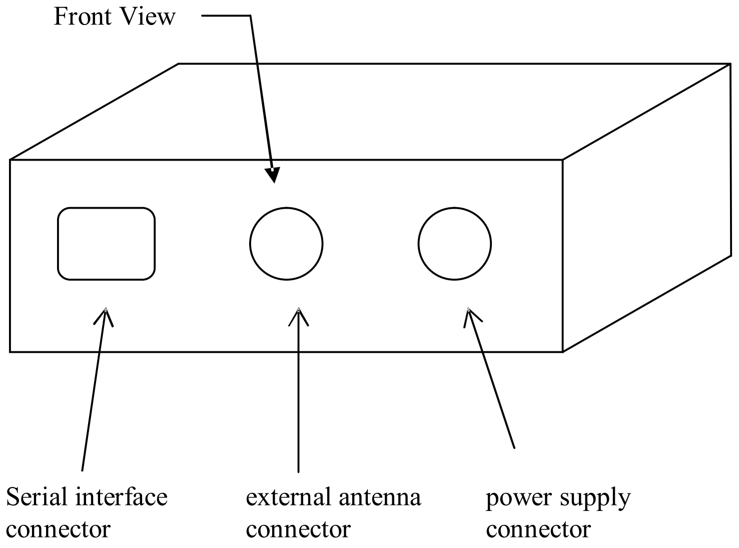
1.2. Specifications

• **Power supply**:	HTEV401	9 - 16 VDC
	HTEV801	+/- 15 VDC
• **Supply current**:	HTEV401	max. 150 mA
	HTEV801	max. +550/-400 mA
• **Frequency**:	125 kHz (optional 134,2 kHz at HTEV901)	
• **Temperature**:	0° - 70° C	
• **Interface**:	RS232	

1.3. Hardware Startup

Metallic environment and electromagnetic interferences (e.g.: monitors, keyboards) have a negative effect on the reading and writing range!

1.3.1. Housing



1.3.2. Connecting the Read/Write Device to your PC and with the Power Supply

Connect the supplied interface cable to the serial interface on your IBM compatible PC. Plug the power supply-cable into a power socket (100-240 VAC at 47-63 Hz).

1.3.3. Connecting the external Antenna

The delivered or user defined antennas may be connected at the external antenna connector. Concerning the design of Long Range antennas please refer to the Antenna design guide delivered from Philips Antenna Design for the HITAG™ Long Range System at http://www.semiconductors.philips.com/acrobat_download/other/identification/ht038713.pdf.

1.4. Software Startup

1.4.1. System Requirements

In order to use the Evaluation Software the following system requirements must be satisfied:

- Intel Pentium 233MHz or higher
- 64 MByte RAM
- serial interface

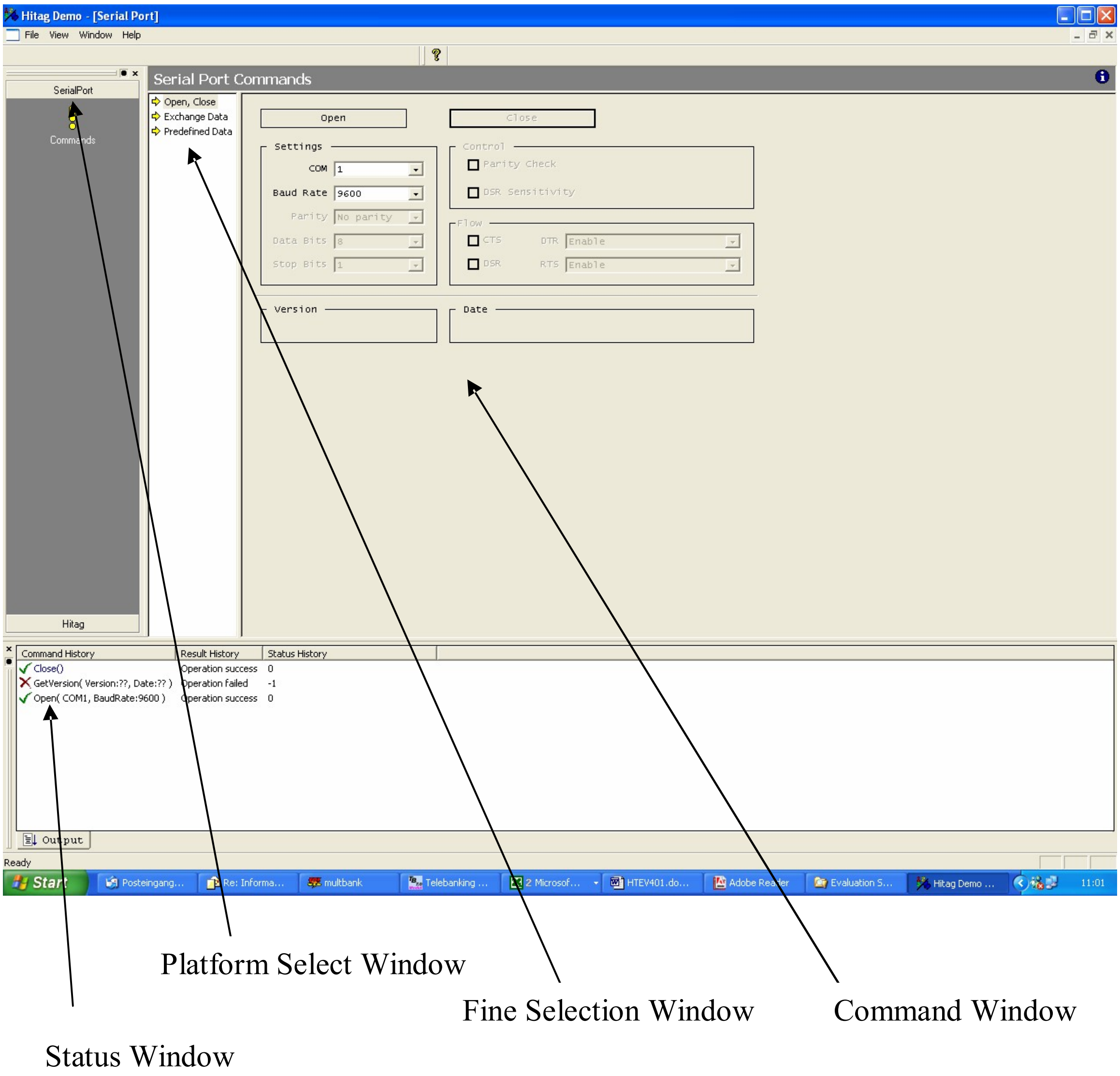
1.4.2. Installation

Start HitagDemoSetup.exe in "HTEV801 CD\Frosch Electronics\Software\EvaluationSoftware" and follow the instructions there. The evaluation software will be installed on your PC

1.4.3. Starting the Demo-Program

Press Start-All programs-Frosch Electronics-HitagDemo-HitagDemo

2. General Definitions for the Demo-Software



COM: 1

Baud Rate: 9600

Parity: No parity

Data Bits: 8

Stop Bits: 1

□ Parity Check

□ DSR Sensitivity

□ CTS DTR: Enable

□ DSR RTS: Enable

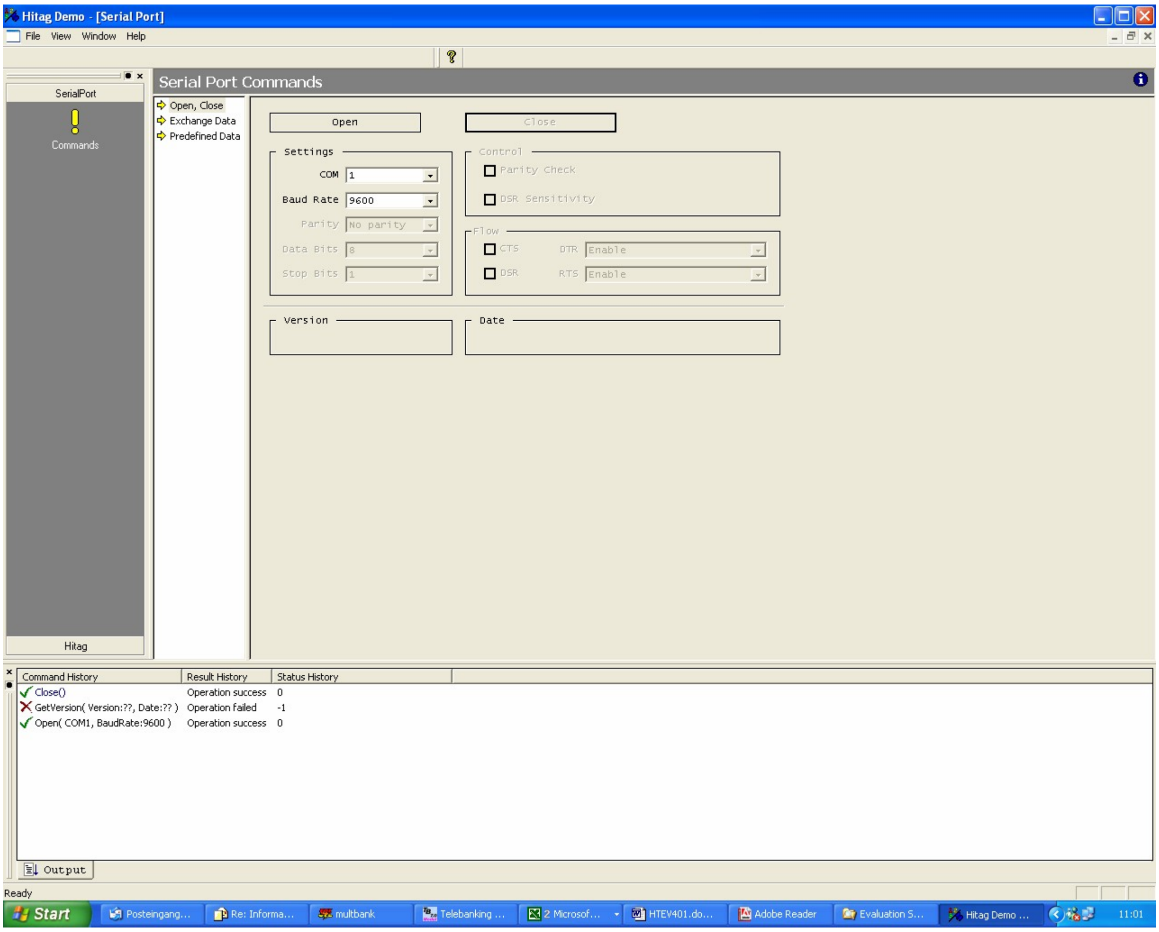
Command History	Result History	Status History
✓ Close()	Operation success	0
✗ GetVersion(Version:??, Date:??)	Operation failed	-1
✓ Open(COM1, BaudRate:9600)	Operation success	0

- Platform Select Window: Choose serial port, reader or transponder specific platform
- Fine Select Window: Subdivision of the Platform
- Command Window: In this window Commands can be send by pressing the specific buttons
- Status Window: displays the serial data transfer

3. Serial Port Menu

3.1. Open/Close

To start communication to the reader you always have to open the port by pressing the "Open" Button. The software opens the port and sends a GetVersion command. For versions higher than 3.xx the software uses the full range of commands (HitagS), for Versions like 2.32 (HTRM400/800 of Philips) or if no reader is detected the software has a limited range of commands (no HitagS Crypto…).

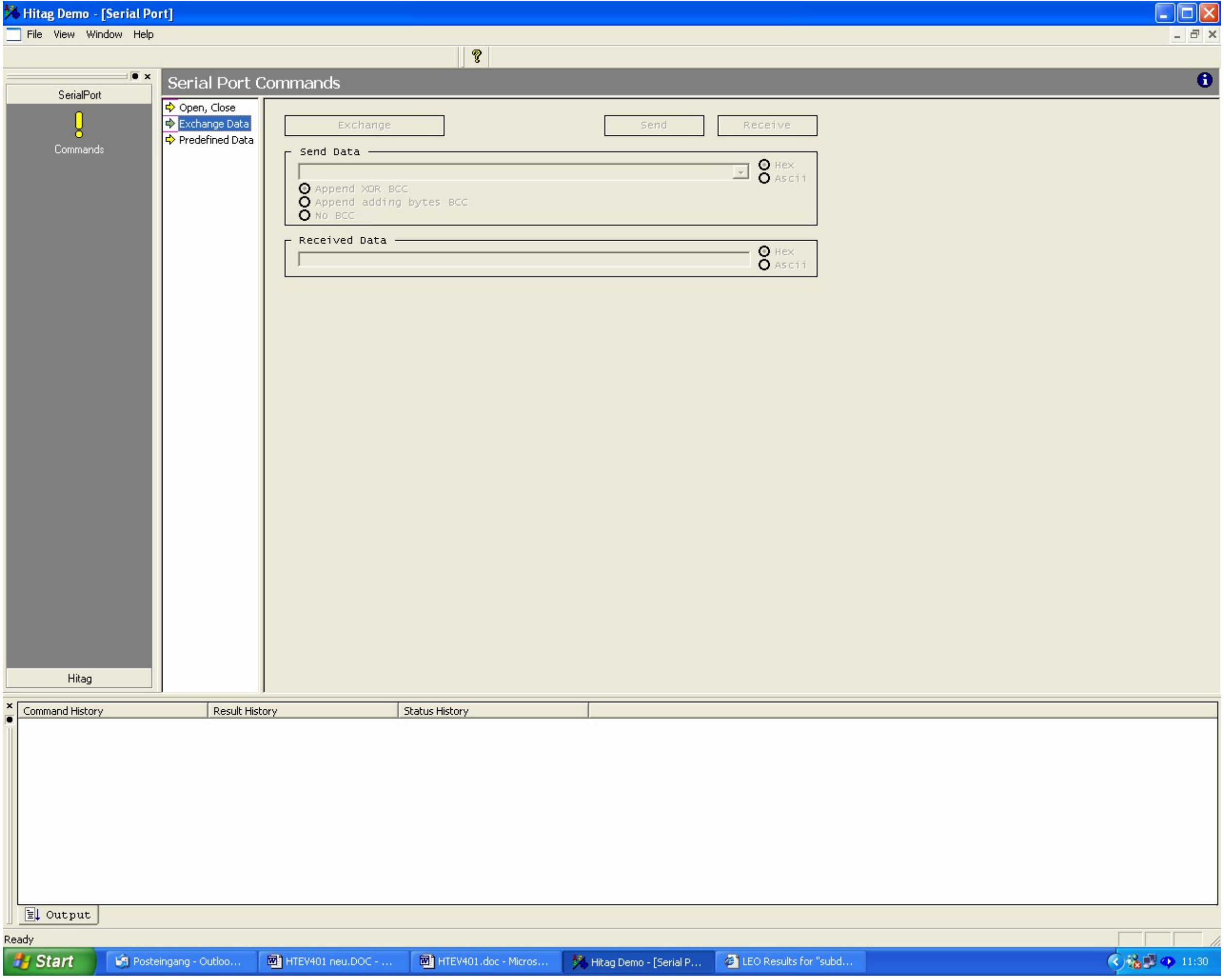


COM: 1
Baud Rate: 9600
Parity: No parity
Data Bits: 8
Stop Bits: 1
DTR: Enable
RTS: Enable

Command History	Result History	Status History
✓ Close()	Operation success	0
✗ GetVersion(Version:??, Date:??)	Operation failed	-1
✓ Open(COM1, BaudRate:9600)	Operation success	0

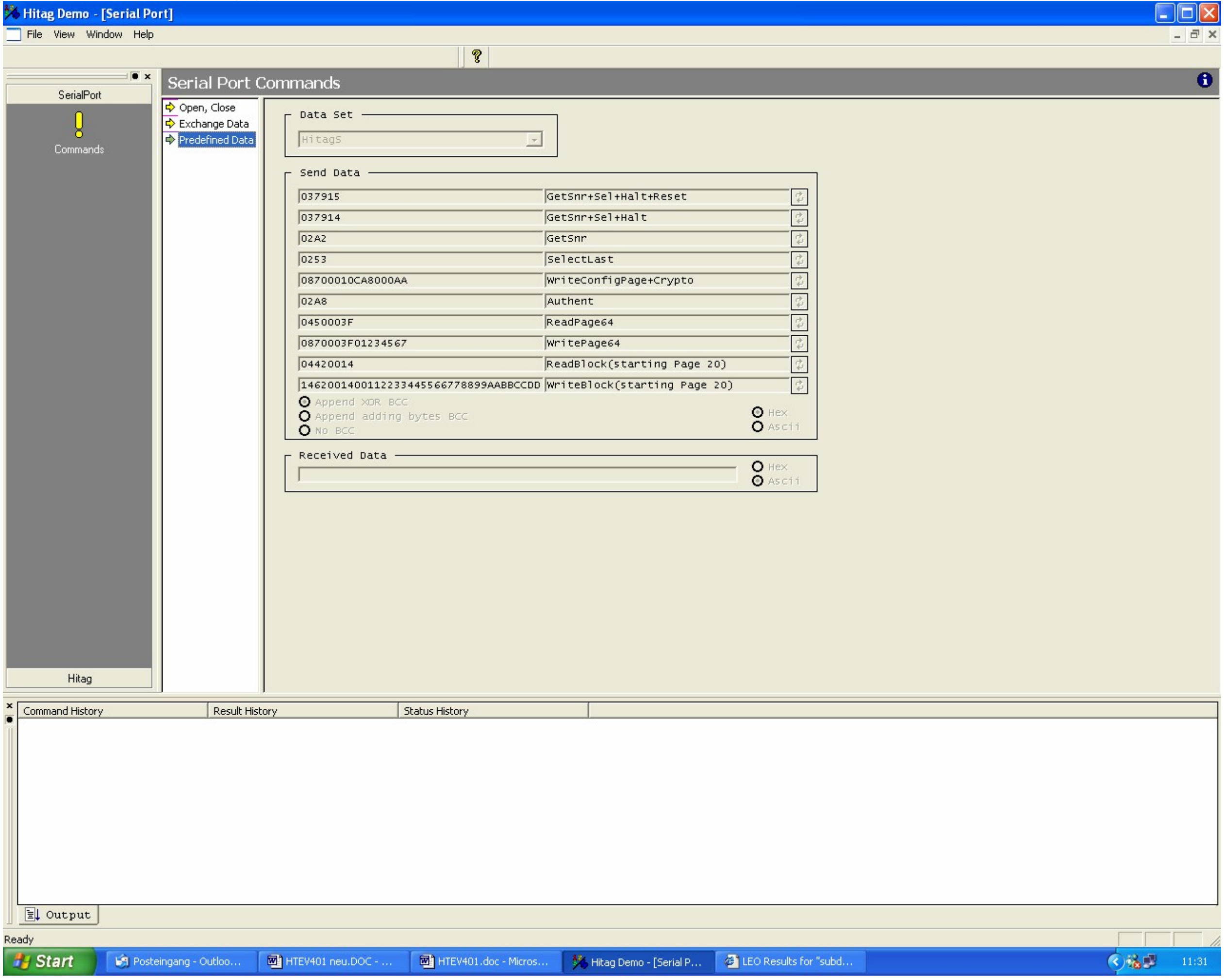
3.2. Exchange Data

User specific commands can be defined and sent in Hex or Ascii format, EXOR, adding or no BCC can be added automatically.



3.3. Predefined Data

Choose out of predefined Data specified in file “HitagDemo.exe.ini”. This file can be modified according your needs



Data Set: HitagS

Send Data

037915	GetSnr+Sel+Halt+Reset
037914	GetSnr+Sel+Halt
02A2	GetSnr
0253	SelectLast
08700010CA8000AA	WriteConfigPage+Crypto
02A8	Authent
0450003F	ReadPage64
0870003F01234567	WritePage64
04420014	ReadBlock(starting Page 20)
1462001400112233445566778899AABBCCDD	WriteBlock(starting Page 20)

● Append XOR BCC
○ Append adding bytes BCC
○ No BCC

● Hex
○ Ascii

Received Data

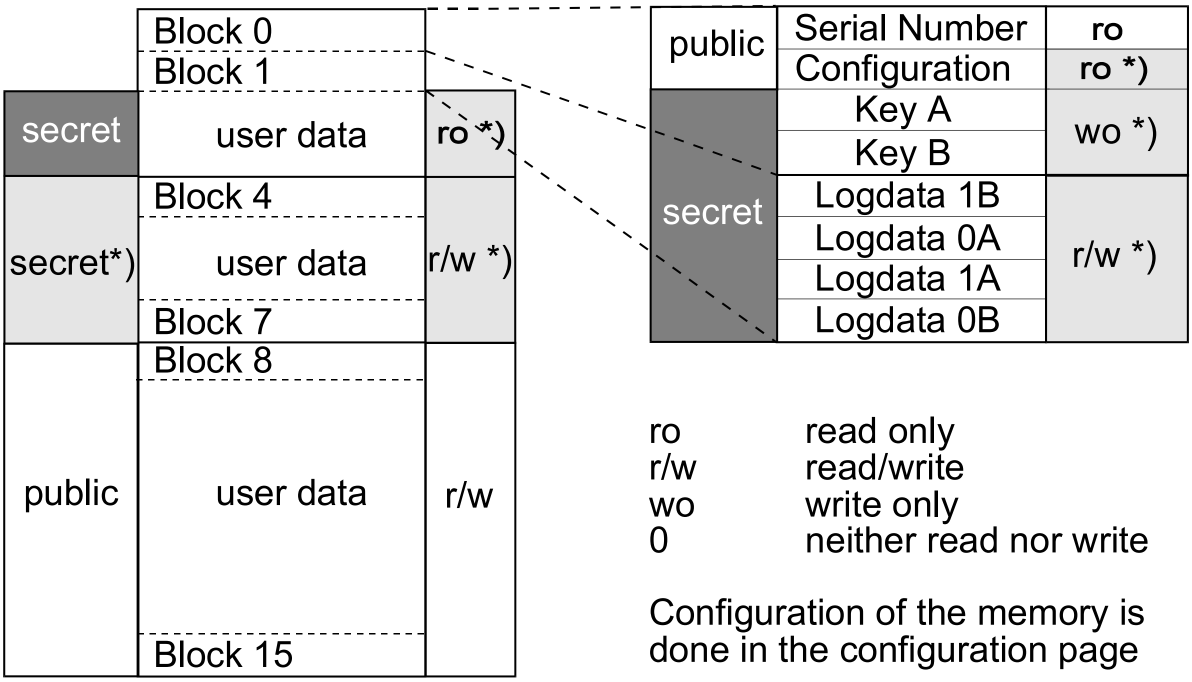
○ Hex
● Ascii

4. HITAG 1 Transponders

4.1. Memory Partitioning

The 2 KBit EEPROM memory on the transponder is divided into 16 blocks. Every block consists of 4 pages with 4 bytes (at 8 bits) each.
Addressing is done page by page and access is gained either page by page or block by block entering the respective start address. In case of block read (or write) the transponder is processed from the start to the end of the block.

The drawing below describes the memory configuration on the Demokit transponder:



ro	read only
r/w	read/write
wo	write only
0	neither read nor write

Configuration of the memory is done in the configuration page

*) **Areas (or settings) marked with an asterisk *) may be configured by the client.**

The memory location described above and marked with an asterisk *) has been configured by Philips, whereby the content of some of the memory areas is free, some allocated.
Block 0 defines the serial number, the configuration of the memory area and the keys, Block 1 the logdata.

Memory locations marked with "secret" can only be accessed after a mutual authentication. An enciphered data communication is used in that area.

Memory locations marked with "public" can be accessed without mutual authentication, no encryption is used.

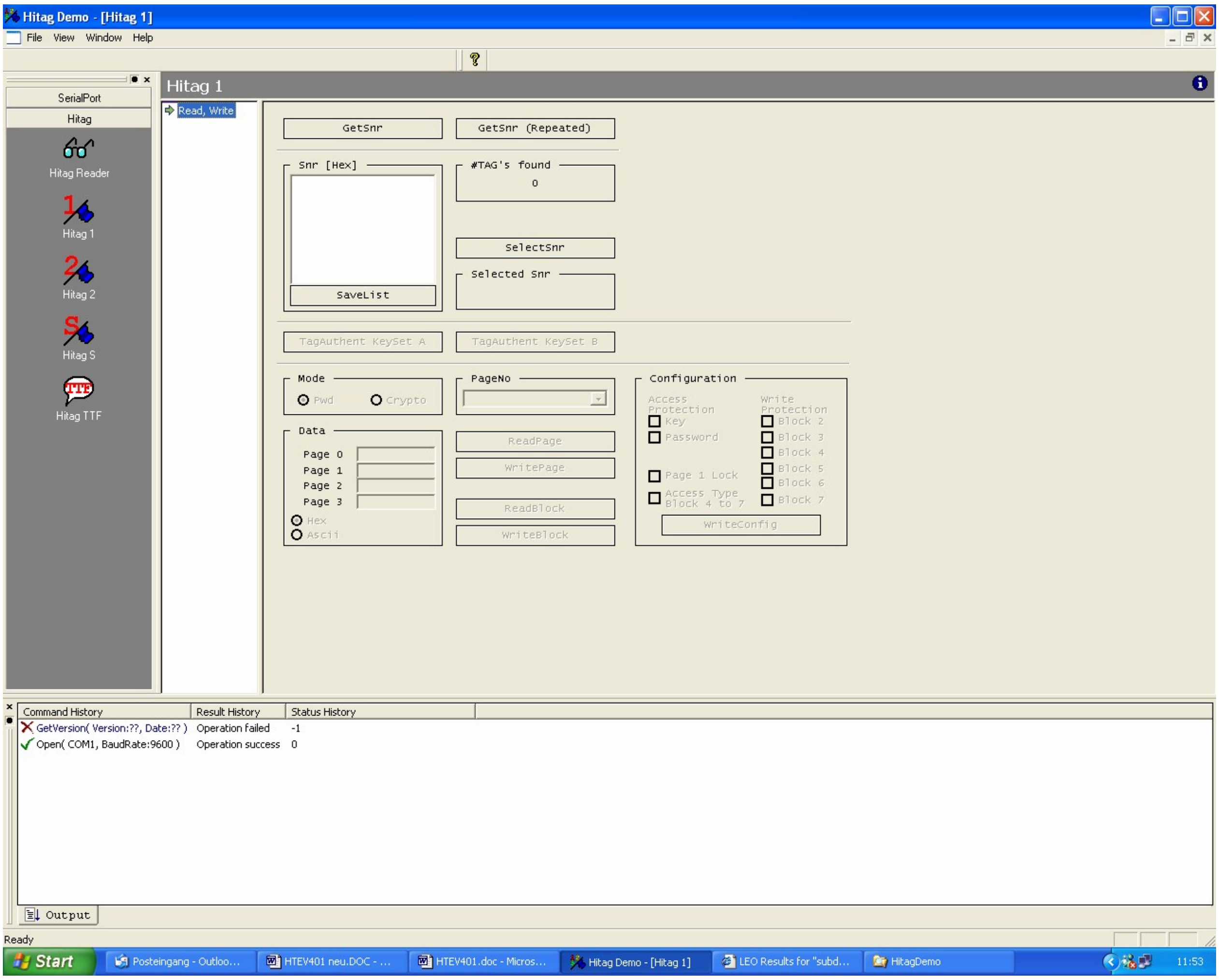
Transponders delivered with this Demokit are configured as follows:
Blocks 4 to 7 of the transponder are public and read-write.

The table shows that the logdata can be both written and read, keys can only be written. That means that keys and logdata can be changed.

Important! You have to be very careful when changing keys and logdata as inconsiderate use results in loss of access to the secret area on the transponder. See Chapter 10 for a detailed description.

4.2. Operating HITAG 1 Transponders

Operating a HITAG 1 transponder the screen will be displayed as follows:



Command History	Result History	Status History
✗ GetVersion(Version:??, Date:??)	Operation failed	-1
✓ Open(COM1, BaudRate:9600)	Operation success	0

4.3. Transponder

Get Snr: Reads the serial numbers of all the transponder located in the field of the antenna. Please be aware that the Long Range kit is not able to perform an anti-collision!

GetSnr (Repeated): Reads the serial numbers of all the transponder continuously, performing a HF Reset at the beginning of each cycle.

SelectSnr: Before it is possible to read or write, one transponder out of the table in the left window has to be selected by marking it with the cursor and pressing the SelectSnr button.

Write Config: After selection of a transponder the current configuration is displayed in this window. The transponder configuration bits can be set or cleared here and the whole page is re-written to the transponder after pressing the button.

Read Page: On entering a page number (0-63) one page (4 bytes) of the transponder is read and displayed on the screen.

Read Block: On entering a page number (0-63) one whole block (15 bytes) of the transponder is read and displayed on the screen, i.e. block 16 for page 61, block 4 if you choose page 16, …..

Write Page: On entering a page number (1-63) and 4 bytes of numbers in the corresponding page this page (4 bytes) is written to the transponder.

Write Block: On entering a page number (4-63) and 16 bytes of numbers in the corresponding block this block (full 16 bytes) is written to the transponder.

TagAuthent: Before sending commands in secret mode, an authentication procedure has to be performed either with key set A or key set B.

Note: You can only write to a page in the corresponding mode public (Pwd) or secret (Crypto)

5. HITAG 2 Transponders

5.1. Memory Partitioning

The memory of the transponder (TAG) consists of 256 bits EEPROM and is organized in 8 pages with 32 bits each. The READ and WRITE instructions always read or write a whole page, and the address transmitted by the base station represents the page address.

Depending on the mode of operation the EEPROM is organized in the following way:

crypto mode:

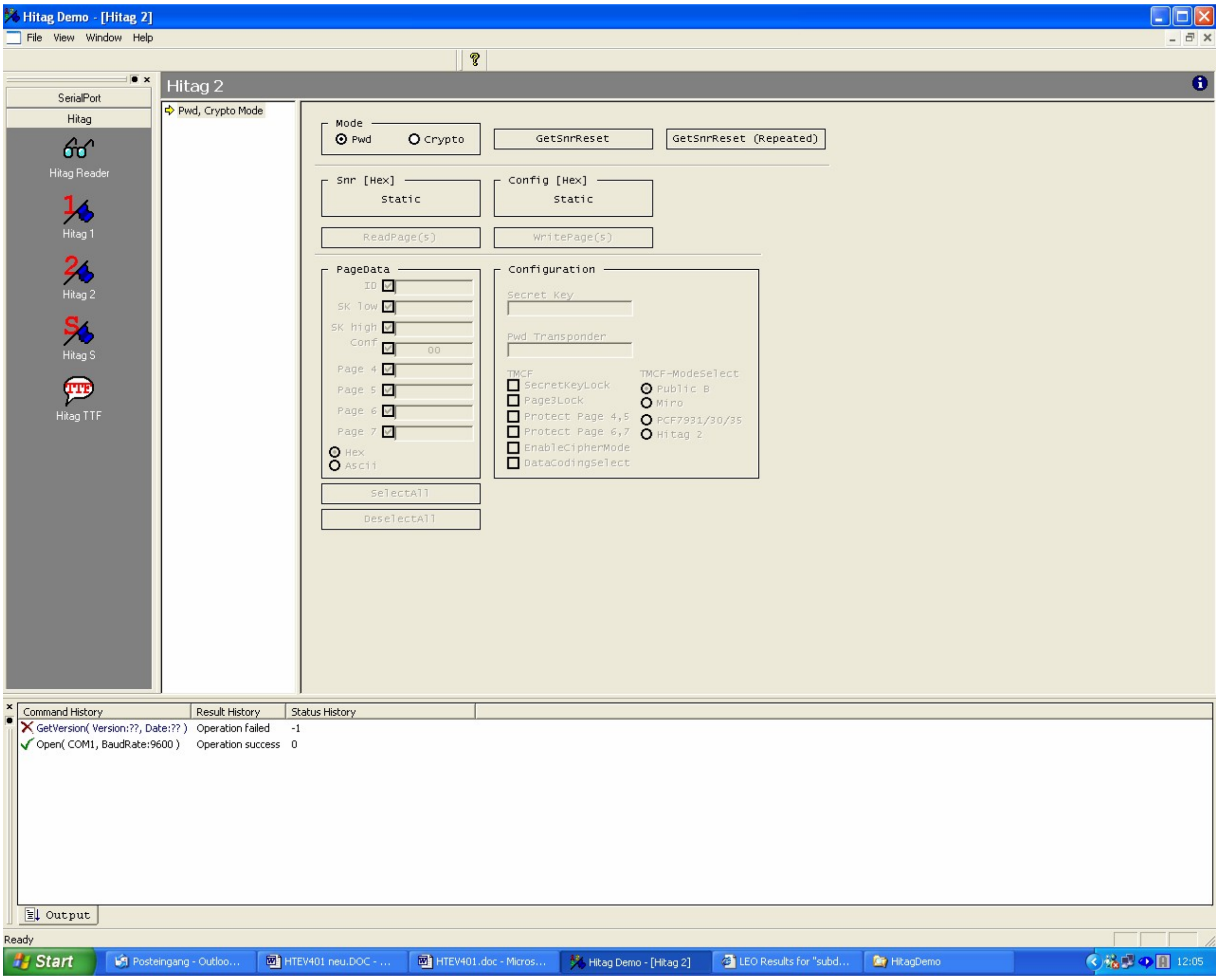
Page	Content
0	ID number
1	32 bit Key: "KEY LOW"
2	16 bit Key " KEY HIGH"
3	8 bit Configuration, 24 bit Password TAG
4	read/write Page
5	read/write Page
6	read/write Page
7	read/write Page

password mode:

Page	Content
0	ID number
1	Password RWD
2	reserved
3	8 bit Configuration, 24 bit Password TAG
4	read/write Page
5	read/write Page
6	read/write Page
7	read/write Page

5.2. Operating Hitag2 Transponders

Operating a HITAG 2 transponder the screen will be displayed as follows:



Mode: ● Pwd ○ Crypto

Snr [Hex]: Static

Config [Hex]: Static

PageData

☑ ID
☑ SK low
☑ SK high
☑ Conf 00
☑ Page 4
☑ Page 5
☑ Page 6
☑ Page 7
● Hex
○ Ascii

Configuration

Secret Key

Pwd Transponder

TMCF
□ SecretKeyLock
□ Page3Lock
□ Protect Page 4,5
□ Protect Page 6,7
□ EnableCipherMode
□ DataCodingSelect

TMCF-ModeSelect
● Public B
○ Miro
○ PCF7931/30/35
○ Hitag 2

Command History	Result History	Status History
✗ GetVersion(Version:??, Date:??)	Operation failed	-1
✓ Open(COM1, BaudRate:9600)	Operation success	0

Ready

Get SnrReset: Reads the serial number of the transponder located in the field of the antenna.

Read Page: Marked pages of the transponder are read and displayed on the screen.

Write Page: Marked pages are written to the transponder.

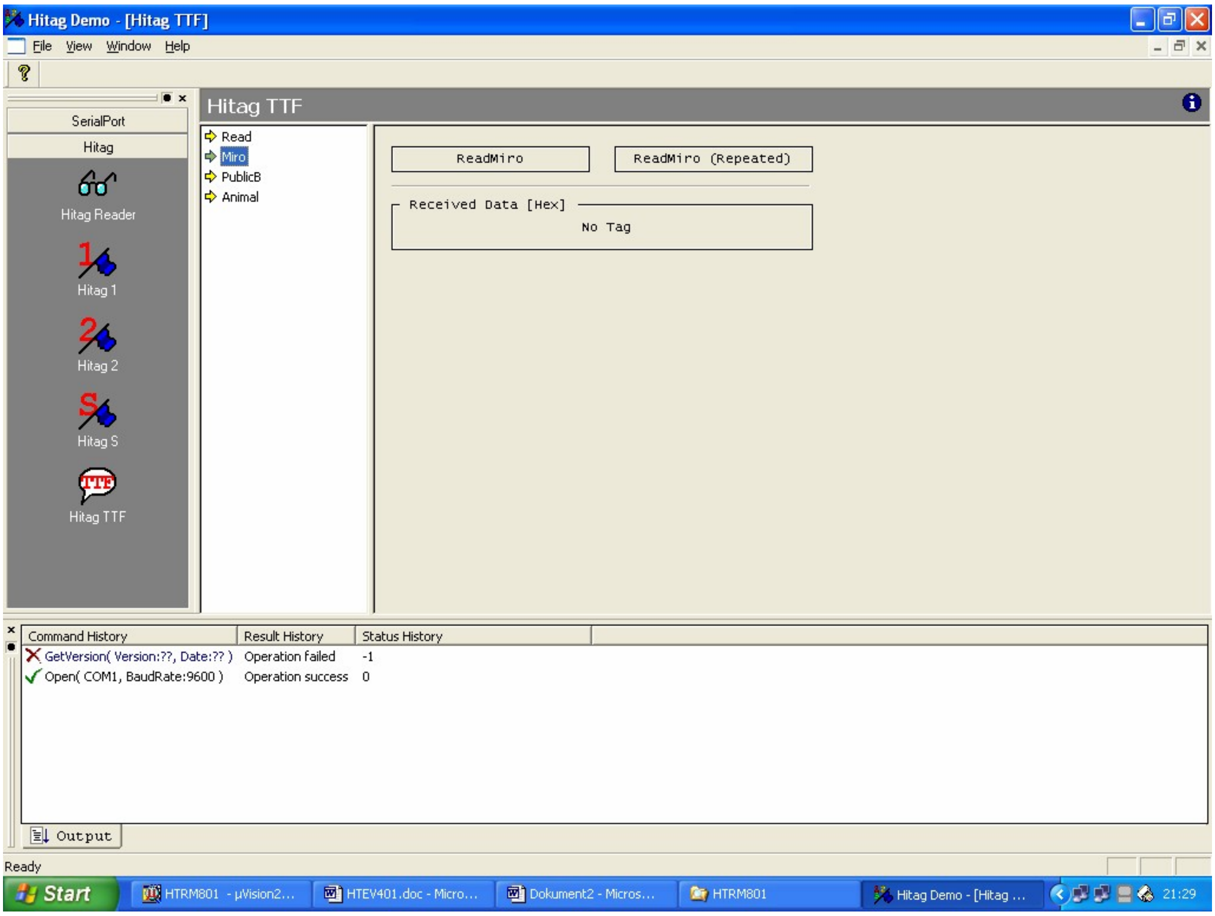
Personalization: Is done in background depending the configuration of the transponder. Gives access to the key and password stored on the transponder (TAG).

- Key is used to encrypt the data sent to and received from the transponder.
- Password TAG is sent from transponder to read/write device and can be verified by the latter depending on the configuration of the read/write device (see also chapter 10)

Configuration: Submenu used to change the configuration of the transponder (see also chapter 9), a write to page 3 has to be performed after changes done in the configuration window

5.3. Public Mode A

Operating a HITAG 2 transponder in Public Mode A the screen will be displayed as follows:

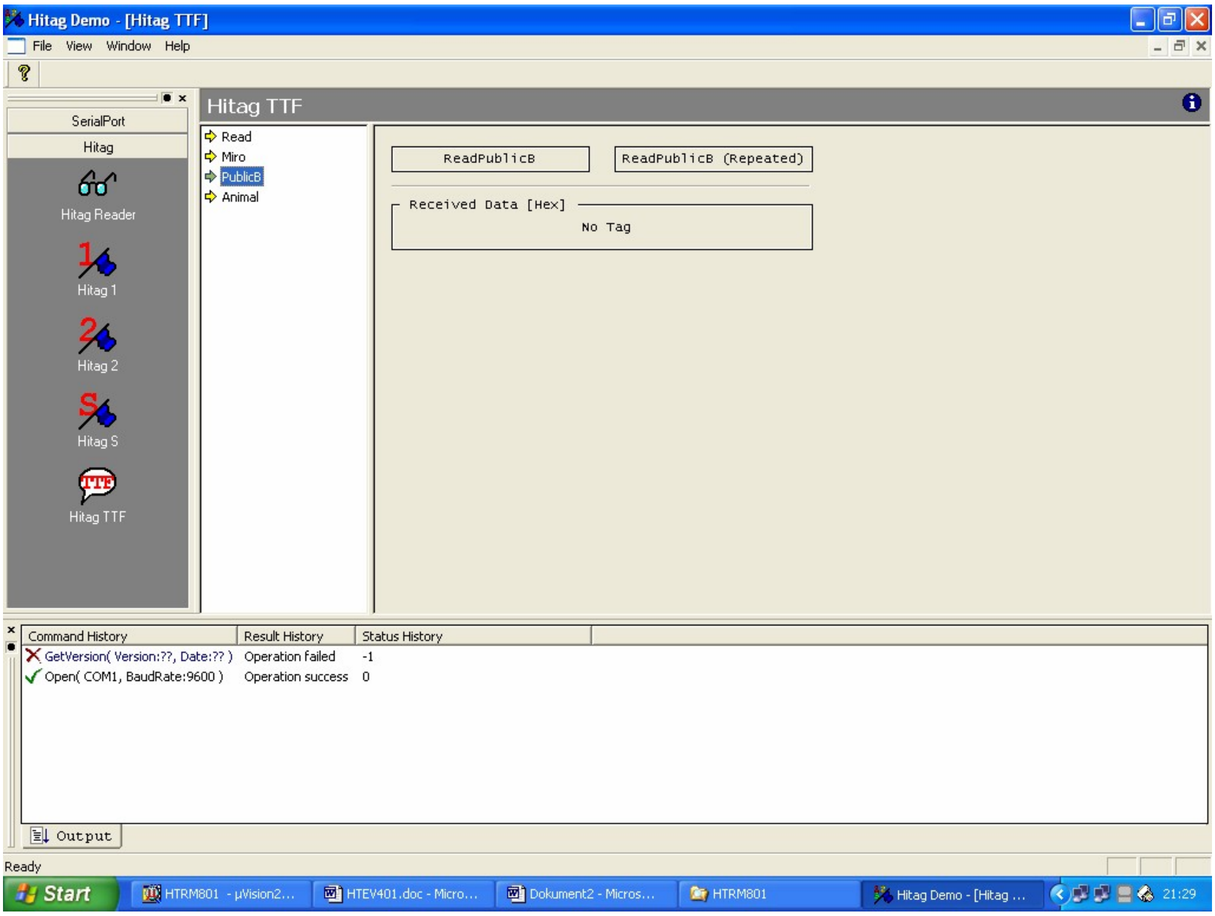


Received Data [Hex]
No Tag

Command History	Result History	Status History
✗ GetVersion(Version:??, Date:??)	Operation failed	-1
✓ Open(COM1, BaudRate:9600)	Operation success	0

5.4. Public Mode B

Operating a HITAG 2 transponder in Public Mode B the screen will be displayed as follows:



```
Received Data [Hex]
                  No Tag
```

Command History	Result History	Status History
✗ GetVersion(Version:??, Date:??)	Operation failed	-1
✓ Open(COM1, BaudRate:9600)	Operation success	0

Ready

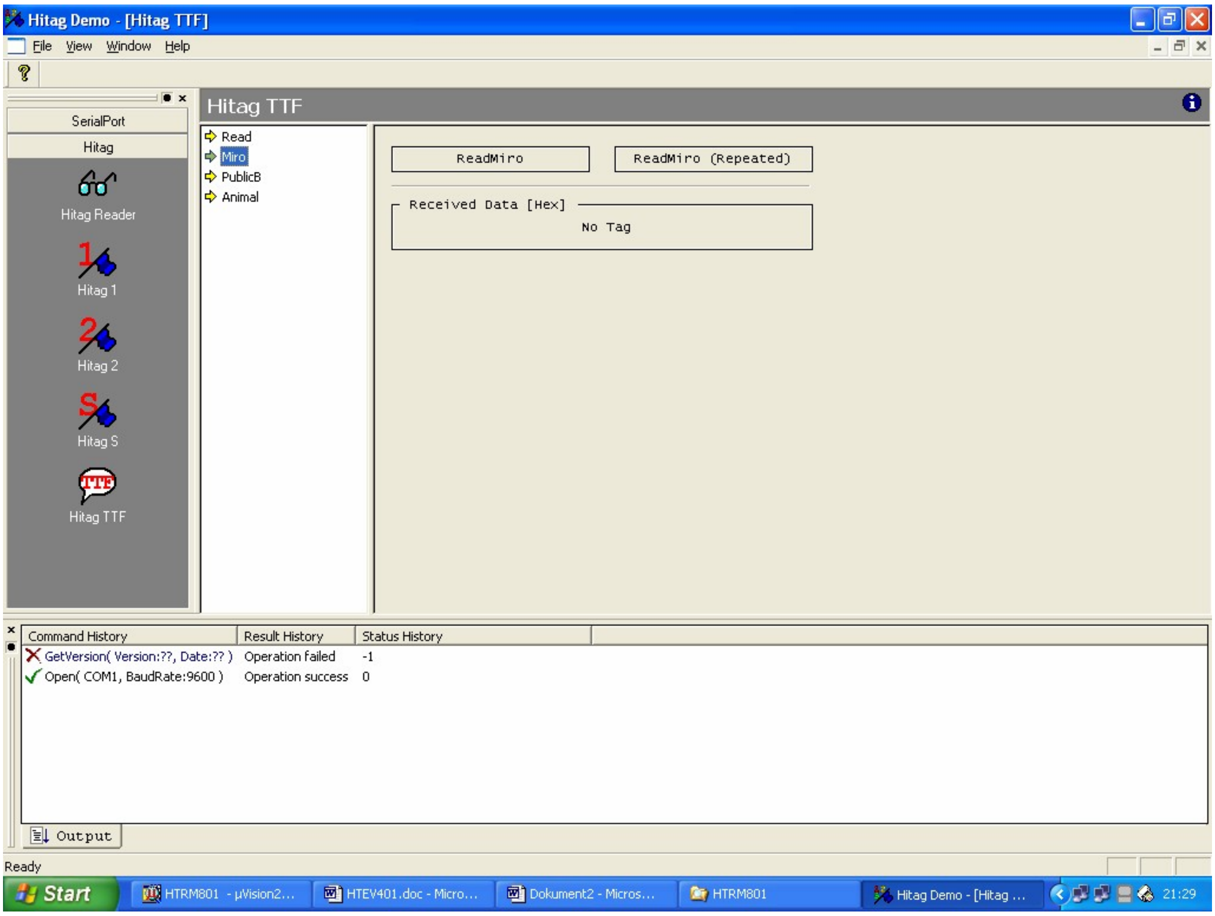
6. MIRO Transponders

6.1. Memory size

In the 64 bit memory the unique 40 bit serial numer of the transponder is stored as well as 24 bits header and parity bits. The data are read only and cannot be changed.

6.2. Operating MIRO Transponders

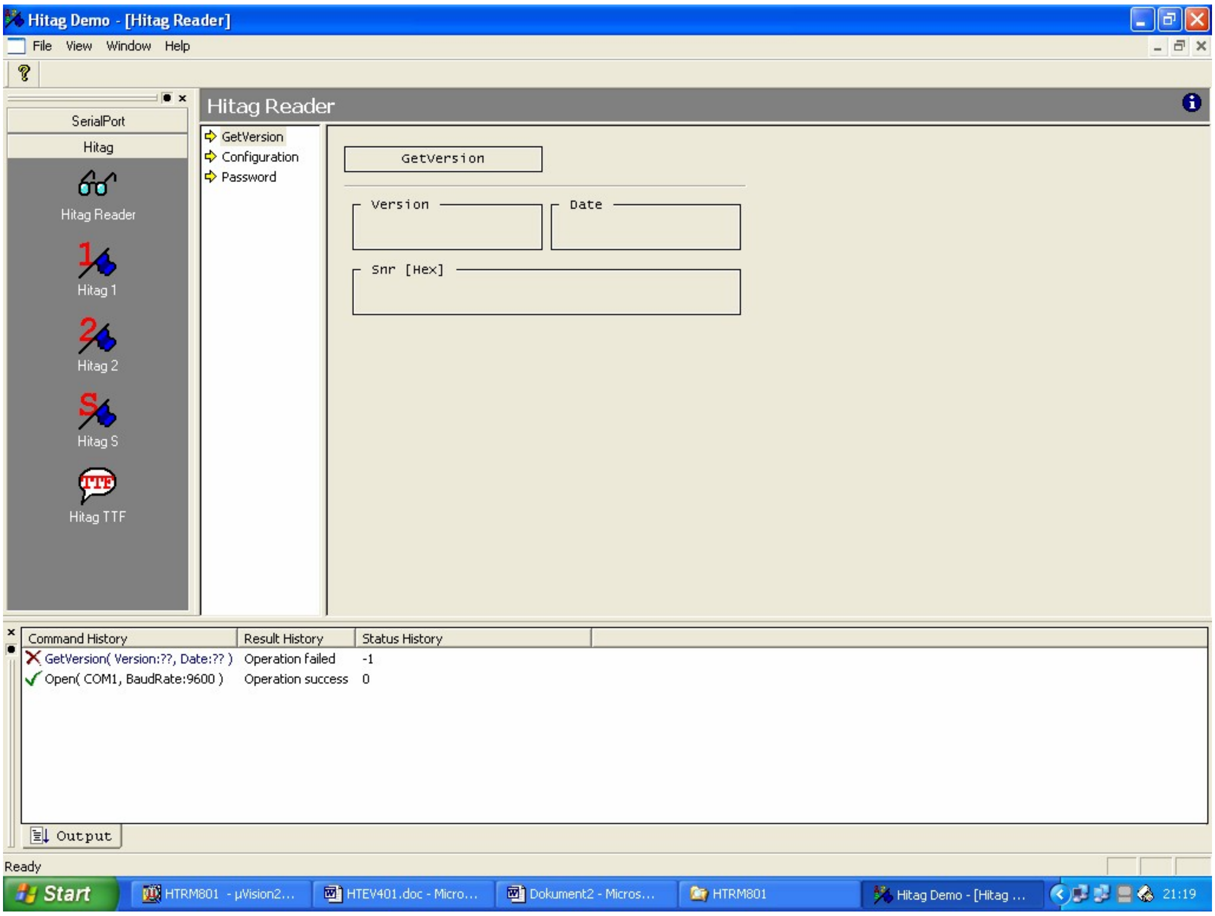
Operating a MIRO transponder the screen will be displayed as follows:



Received Data [Hex]
No Tag

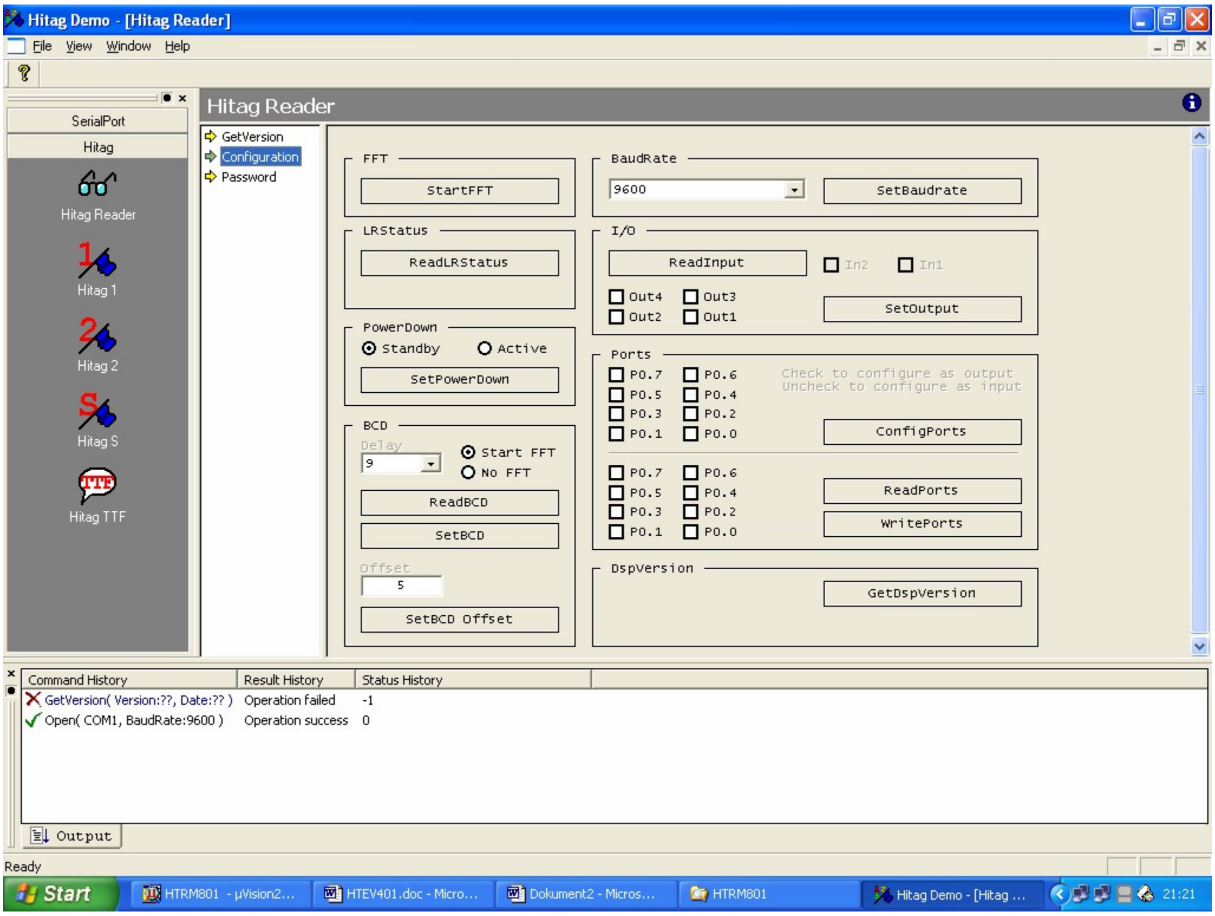
Command History	Result History	Status History
✗ GetVersion(Version:??, Date:??)	Operation failed	-1
✓ Open(COM1, BaudRate:9600)	Operation success	0

7. R/W-Device



Command History	Result History	Status History
✗ GetVersion(Version:??, Date:??)	Operation failed	-1
✓ Open(COM1, BaudRate:9600)	Operation success	0

Get Version: Reads the version and programming date of the firmware and the serial number of the Core Module.



PowerDown: ● Standby ○ Active

BaudRate: 9600

I/O: □ In2 □ In1 □ Out4 □ Out3 □ Out2 □ Out1

Ports: □ P0.7 □ P0.6 □ P0.5 □ P0.4 □ P0.3 □ P0.2 □ P0.1 □ P0.0

□ P0.7 □ P0.6 □ P0.5 □ P0.4 □ P0.3 □ P0.2 □ P0.1 □ P0.0

BCD: Delay 9 ● Start FFT ○ No FFT

Offset 5

Command History	Result History	Status History
✗ GetVersion(Version:??, Date:??)	Operation failed	-1
✓ Open(COM1, BaudRate:9600)	Operation success	0

StartFFT: This command starts the Fast Fourier Transformation (FFT) of the Digital Signal Processor. This command is to be used as often as required depending on the noisefloor of the environment. Note that no TTF transponder is in the field when starting FFT

ReadLRStatus: This command can be used to check the antenna status (broken or badly detuning antennas can be detected).

Set PowerDown: Antenna drivers can be switched on or off.

Set BCD: This command adjusts the timing of the read/write device to the antenna. The command has to be operated once, when an antenna is connected for the first time or changed, it can be done with or without successing FFT.

SetBaudRate: Baudrates from 9600 to 57600 kHz can be chosen, be aware that after a power reset the Baudrate switches back to 9600.

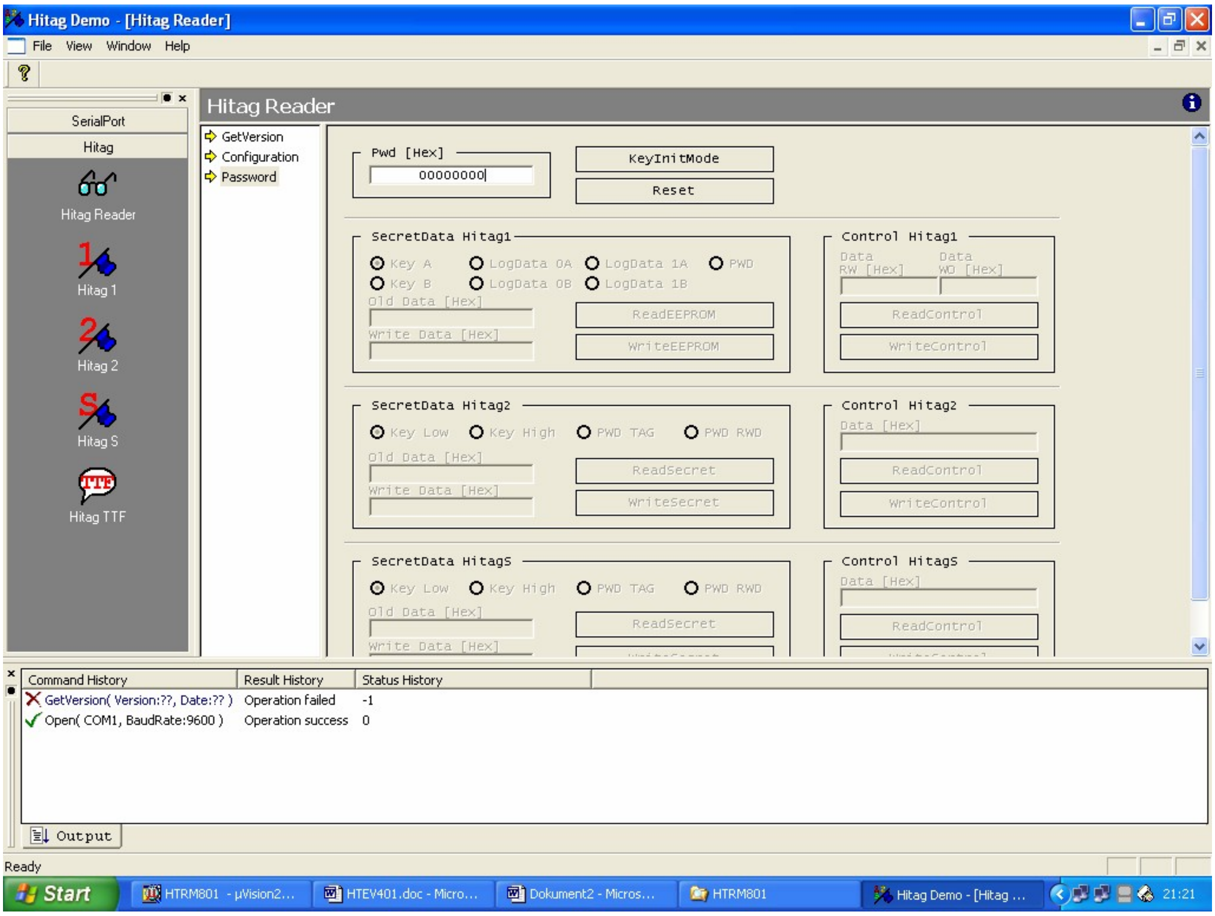
SetOutput: Out1-4 can be cleared or set, only Out1 is available at the HTRM801.

ReadInput: Read status of In1/2.

Port Commands: Not in use.

DSP Version: Not in use.

*) The commands **Fast Fourier** and **Set BCD** are only enabled when using HITAG Long Range Read/Write Devices.



Pwd [Hex]: 00000000

Command History	Result History	Status History
✗ GetVersion(Version:??, Date:??)	Operation failed	-1
✓ Open(COM1, BaudRate:9600)	Operation success	0

KeyInitMode: This command is necessary to get access to the secret keys that are stored in the EEProm of the Core Module and that are used for Authenticate the transponders.

8. Error Messages

Error messages and the message ***function OK*** are displayed in the status line.

- Function OK System is working correctly.
- Serial error Error on the serial interface.
- NOTAG There is no transponder in the communication field of the antenna
  or a not initialized HT2 Public A or B is in the communication field of the antenna
  or a HT2 Crypto was accessed using the wrong key.
- TIMEOUT error There is not enough energy to write to the transponder.
- AUTHENT error An error occured during the authentication process.
- QUIT error The acknowledgement was not received correctly.
- CRYPTO not initialized A cryptographic command was transmitted without authentication.
- HT2 authentication error No conformity between password RWD stored in the read/write device and password RWD stored on the transponder,
  or a HT2-Crypto Tag was accessed using the Password mode.
- incorrect password TAG No conformity between password TAG stored in the read/write device and password TAG stored on the transponder.
- EEPROM error Read/write device EEPROM check sum error.
- EEPROM wrong old data On comparison old and new data (for keys and passwords) prove inconsistent.
- EEPROM write protected Parts of the EEPROM on the read/write device were locked using the configuration menu and a write access to this part was tried.
- EEPROM read protected Parts of the EEPROM on the read/write device were locked using the configuration menu and a read access to this part was tried.

9. Configuration of hitag™ Transponders

9.1. Security Mechanism

All the data necessary for the authentication of the transponder and the read/write device as well as data needed for encryption can be protected from being read and from being written on the read/write device using special commands.

This mechanism has 3 levels:

Level 0: All security relevant data can be read and written.

Level 1: The data cannot be read any more. If you want to change an entry, you have to know the old value. Otherwise writing access will be denied.

Level 2: The internal data are locked and can neither be read nor written. At this level it is impossible for the user to change the stored data.

The following data are subject to the mechanism described above:

- Key information A and B
- Logdata 0A, 0B
- Logdata 1A, 1B

} for HITAG 1 transponders

- Key information
- Password TAG
- Password RWD

} for HITAG 2 transponders

You cannot reset levels, e.g. from level 2 to level 1. Once a security level has been chosen it becomes irreversible.

If you want to write the key and passwords to or read them from the read/write device you have to enter the KeyInit Password.

If you do not know this password, you will not be able to enter the personalization and configuration submenus of the read/write device as you cannot read this password from the read/write device.

To change the KeyInit Password you have to know the current value.

The default password is set to 0x00000000 by Philips.

After entering the correct KeyInit Password access to the personalization and configuration submenus of the read/write device is granted.

10. Personalizing your Read/Write Device and the Transponders

Note: It is NOT NECESSARY to personalize the read/write device and the transponders in order to operate the Evaluation Kit!
A pre - personalization was done by Philips.

In order to profit from the full functionality of the HITAG system, the Evaluation Kit, however, supports all cryptographic features.

This requires the use of some secret data (keys, logdata and passwords). The process of **loading these data** into the **read/write device** is called **personalization**. The same personalization procedure has to be carried out on your transponders. The read/write device and the transponders are personalized by Philips by means of defined **Transport Keys, Transport Logdata** and **Transport Passwords** (HITAG 1 Keys and Logdata are set to 0x00000000, HITAG 2 Key is set to 0x4D494B524F4E, HITAG 2 Password TAG to 0xAA4854 and HITAG 2 Password RWD to 0x4D494B52).
Therefore you can operate the Evaluation Kit without changing any data. If you want to use own keys, logdata or passwords you have to personalize read/write device and transponders as it is described in the following chapters.

Make sure you are in a safe environment while writing secret data to the transponder or the read/write device. This prevents possible listening in to the communication between HOST and read/write device.

On the next few pages you find a description of how to personalize your read/write device. In Chapter 10.3. the loading of own keys, logdata and passwords into the read/write device and the transponder is described in exact order.

10.1. General Definitions

In order to be able to read data from the secret area of a transponder, you have to carry out a procedure called authentication. To do this you need special data (keys).
After transmitting the according command the authentication is automatically carried out by the HITAG Read/Write Device.

10.1.1. HITAG 1 Transponders

10.1.1.1. Definition of the Keys

Keys are cryptographic codes, which determine data encryption during data transfer between read/write device and transponder.
Two keys (Key A and Key B) which you can use independently of each other, have been installed for security and flexibility reasons. The identity of either Key A or Key B on the read/write device and on the transponder is sufficient (see table under 10.1.1.2.).

The keys are predefined by Philips by means of defined Transport Keys (both keys show the same bit map). They can be written only.

10.1.1.2. Definition of the Logdata

Logdata represent "passwords" needed to gain access to secret areas on the transponder. A pair of logdata is included with every cryptographic key (Key A and Key B). This logdata pair has to be identical both on the transponder and the read/write device.

ad Key A:	Logdata 0 A	"Password" which the transponder sends to the read/write device and which is verified by the latter.
	Logdata 1 A	"Password" which the read/write device sends to the transponder and which is checked for identity by the latter.
ad Key B:	Logdata 0 B and Logdata 1 B	analogous to Key A

The logdata are also predefined by Philips using defined Transport Logdata (all logdata show the same bit map). They can be read and written. Logdata 0A and 1A, as well as Logdata 0B and 1B do not have to show the same values, but all Logdata have to be identical on the read/write device and on the transponder!

So it is important that the following values are in accordance with each other, i.e. the respective data on the read/write device and on the transponder have to be identical pairs:

on the read/write device		**on the transponder**	
KEY A	⇔	KEY A	Set A
LOGDATA 0A	⇔	LOGDATA 0A	
LOGDATA 1A	⇔	LOGDATA 1A	
KEY B	⇔	KEY B	Set B
LOGDATA 0B	⇔	LOGDATA 0B	
LOGDATA 1B	⇔	LOGDATA 1B	

Attention: **Keys and Logdata only can be changed if the Transport Keys and the Transport Logdata are known!**

10.1.2. HITAG 2 Transponders

10.1.2.1. Definition of the Keys

Keys are cryptographic codes, which determine data encryption during data transfer between read/write device and transponder.

The key is predefined by Philips by means of a defined transport key.

10.1.2.2. Definition of the Passwords

Passwords are needed to gain access to the transponder. A pair of passwords is stored in every transponder. This password pair has to be identical both on the transponder and the read/write device.

Password TAG: Password that the transponder sends to the read/write device and which may be verified by the latter (depending of the configuration of the read/write device).

Password RWD: Password that the read/write device sends to the transponder and which is checked for identity by the latter.

The passwords are also predefined by Philips using defined transport passwords. They can be read and written. *Password TAG* and *Password RWD* do not have to show the same values, but all passwords have to be identical on the read/write device and on the transponder!

The passwords are predefined by Philips by means of defined transport passwords.

So it is important that the following values are in accordance with each other, i.e. the respective data on the read/write device and on the transponder have to be identical pairs:

on the read/write device		**on the transponder**
KEY	⇔	KEY
Password TAG	⇔	Password TAG
Password RWD	⇔	Password RWD

10.2. Personalization Concept

To enable utmost security and flexibility Philips worked out a personalization concept that shall be shortly described in the following:

The first stage is a test that is done by the producer respectively Philips. Here the unique serial number is fixed and transport keys and transport passwords are pre-programmed.
In the next stage the customers program their own keys and passwords (so nobody besides them can access the transponders) and configure the memory of the transponders. We recommend to lock sensitive areas, that means for example to prevent the possibility to change keys and passwords for the user.
In the last stage the user just reads from and writes to the memory of the transponders.

10.3. Changing Keys and Passwords

You can change keys and passwords using the menu options in the **personalization** submenu for the read/write device and for the transponders. You have to be careful when carrying out such a change.
Entering the personalization submenu for the read/write device requires a password you have to enter only once when running the demosoftware. The default password is set to **0x00000000** by Philips.

You do <u>not</u> have to change this data in order to operate the Demonstration Kit!

<u>If you want to change keys and passwords, please, strictly follow the steps below:</u>

- ***Set Transponder Access to Single access! (See chapter 3.1)***
- ***Place transponders one after the other directly on the antenna or hold them directly to it! (0-distance)***

10.3.1. HITAG 1 Transponders

10.3.1.1. Changing Keys

Please, note the order of the steps!

1. Access the transponder (using the Transport Keys).
2. Change a key (e.g.: Key A) on the transponder, i.e., using transponder personalization submenu, see chapter 4.3.
3. Change Key A on the read/write device to the new value (using the Personalization submenu, see Chapter 4.4).

Caution: On the transponder the key can only be written, which means that you cannot call up the entry! Moreover, you need to know the old value if you want to change the key on the read/write device! (If you enter wrong values the message *Wrong old data* is displayed.)

Only after carrying out correctly steps 1 through to 3 may the second key be changed following the steps described above. Conveniently you change both keys to the same value!

10.3.1.2. Incorrect Procedures Changing Keys

- You change both keys on the read/write device and then try to access the transponder. This is not possible (the status line displays the message *Authentication error*) because there is no identity between any of the keys on the transponder and the read/write device.
- You change only one key (e.g.: Key A) on the read/write device; the second key (in this example B) remains the Transport Key. Then you try again to access the transponder. In this case you will gain access because one key (here it is Key B) on the transponder and the read/write device is still identical. Therefore, the status line briefly displays the message *Authentication error* (after the first failed attempt to gain access using the changed key) then the message *Function OK* appears.

The same scenario applies if you first change one or both of the keys on the transponder but leave the keys on the read/write device unchanged (transport keys).

10.3.1.3. Changing Logdata

Change logdata using the same procedure as described for changing keys. Be careful to change them by pairs (on the read/write device and on the transponder):

1. Change, for example, Logdata 0A on the transponder (by overwriting Page 5).
2. Change Logdata 0A on the read/write device to the new value.
3. Change Logdata 1A on the transponder (by overwriting Page 6).
4. Change Logdata 1A on the read/write device to the new value.

Again, you need to know the old values before they can be changed on the read/write device. Therefore, we recommend that you use a table to record changed keys and logdata during the first phase of getting to know the system!

When you change a key, this does not mean that you also have to change the corresponding logdata and the other way round.

10.3.2. HITAG 2 Transponders

10.3.2.1. Changing the Key

Please, note the order of the steps!

1. Access the transponder in crypto mode (using the Transport Key).
2. Change the key on the transponder, using the transponder personalization submenu (see chapter 5.2.1). You do not need to change the password.
3. Change the key on the read/write device to the new value (using the RW-Device personalization submenu, see chapter 5.2.2).

Only after carrying out correctly steps 1 through to 3 the transponders are accessible with the new key.

10.3.2.2. Incorrect Procedures Changing the Key

- You change the key on the read/write device and then try to access the transponder. This is not possible (the status line displays the message *NOTAG*) because there is no identity between the keys on the transponder and the read/write device.

The same scenario applies if you first change the key on the transponder but leave the key on the read/write device unchanged (transport key).

10.3.2.3. Changing Passwords

Change passwords using the same procedure as described for changing the key. Be careful to change them by pairs (on the read/write device and on the transponder).

1. Access the transponders in password mode.
2. Change one Password (e.g.: *Password TAG*) on the transponders using the transponder personalization submenu (see chapter 5.3.1).
3. Change *Password TAG* on the read/write device to the new value (using the RW-Device personalization submenu, see chapter 5.3.2).

Only after carrying out correctly steps 1 through to 3 (executing a read-access test the message **Function OK** has to be displayed in the status line) may the second password be changed following the same steps described above.

When you change e.g. *Password TAG*, this does not mean that you also have to change *Password RWD* and the other way round.

10.3.2.4. Incorrect Procedures Changing Passwords

- You change the *Password RWD* on the read/write device and then try to access the transponder. This is not possible (the status line displays the message *incorrect Password RWD*) because there is no identity between the *Password RWD* on the transponder and on the read/write device.
- You change the *Password TAG* on the read/write device and then try to access the transponder. This is not possible (the status line displays the message *incorrect Password TAG*) because there is no identity between the *Password TAG* on the transponder and on the read/write device. This only applies, if you enabled checking of the *Password TAG* (see chapter 9.3.1) in the read/write device.

The same scenario applies if you change the passwords on the transponders but leave the passwords on the read/write device unchanged (transport passwords).

11. Ordering Information

Type Name	Description	Ordering Number
HTEV401	HITAG Proximity Evaluation Kit 125 kHz	E31003
HTEV801	HITAG Long Range Evaluation Kit 125 kHz	E31001
HTEV901	HITAG Long Range Evaluation Kit 134,2 kHz	E31002

Frosch Electronics OEG

Customized RFID Solutions

Münzgrabengürtel 10
8010 Graz
Austria

Tel.:	+43 697055/0
Fax:	+43 697055/12
mail to:	info@froschelectronics.com

www. froschelectronics.com

The information presented in this document does not form part of any quotation or contract, is believed to be accurate and reliable and may be changed without any notice. No liability will be accepted by the publisher for any consequence of its use. Publication thereof does not convey nor imply any license under patent- or other industrial or intellectual property rights.