BOURGOGNE ET GRASSET

Vegas Readers

User Manual

July 2002

BASIC VERSION : 2 VEGRDE2

CONFIDENTIAL

PHILIPS

Bourgogne et Grasset — ZI Beaune Savigny — 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

Table of Contents

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

Due to future technical developments this description is subject to change without notice.

This document was set up with great care. In the case of possible damage resulting from incorrect information in this description the client is not entitled to take action for damages.

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

1. Introduction

The VEGAS read/write unit (VersionVEGRDE2) handles the communication with all electronic units designed for gaming purpose in order to guarantee a stable identification of at least 20 special gaming chips within one antenna. Each special gaming chip, in future called Jeton, includes a HITAG VEGAS electronic unit designed for this application.

During a gaming cycle a memory access applies to each selected and identified Jeton in order to read the stored gaming balue from definite memory address. The memory read-command can be done either block- or page wise.

The VEGAS read/write unit (VersionVEGRDE3) offers following basic features:

- 125 kHz carrier (international standard)
- reading and writing of HITAG VEGAS data carriers
- high security by using cryptography, mutual authentication and password verification
- several interfaces (RS232, CMOS)
- highest EMC and EMI standards
- operation of several data carriers simultaneously
- antenna multiplex possible by adding only few components
- easy way for antenna design
- easy system integration
- software controlled standby mode
- software controlled input and output for general purposes
- antenna malfunction indication

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

2. Data Carriers

2.1. HITAG Data Carriers

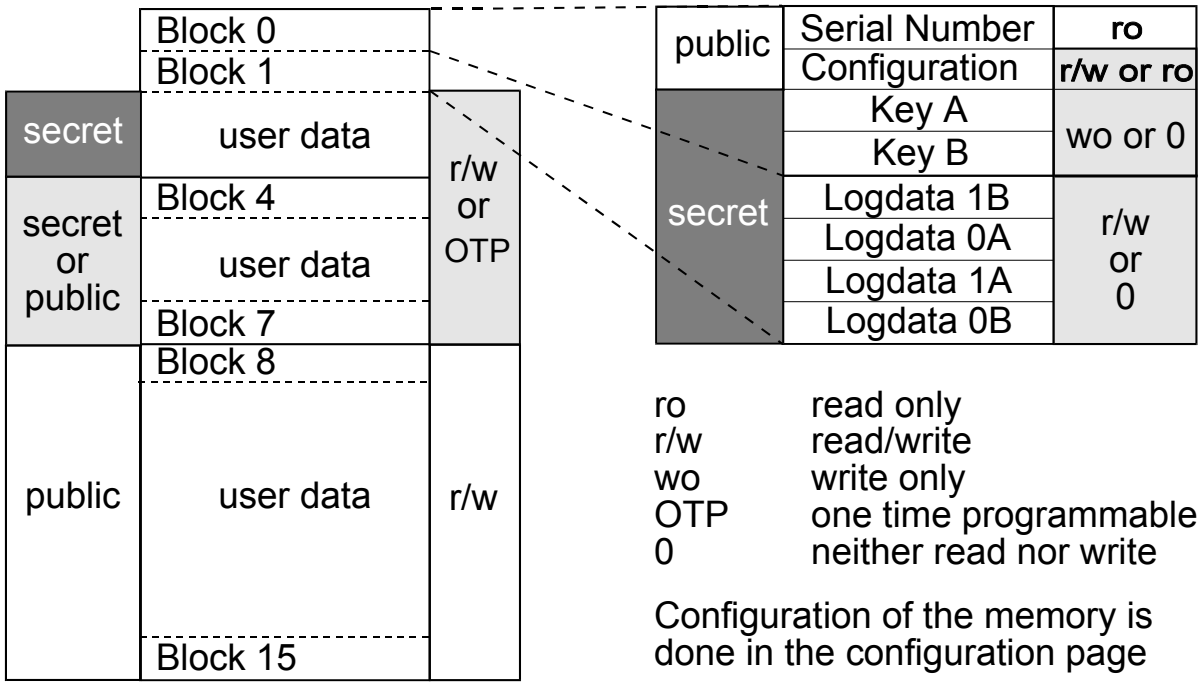
2.1.1. Memory Structure of the Data Carrier

The 2 KBit memory area in the EEPROM of the data carrier is divided into 16 blocks. Each block comprises 4 pages with 4 bytes (at 8 bits) each.
Addressing is done page by page (page 0 .. 63) and access is gained either page by page or block by block entering the respective start address (page number). In case of block read/write the data carrier is accessed from the start address to the end of the block.

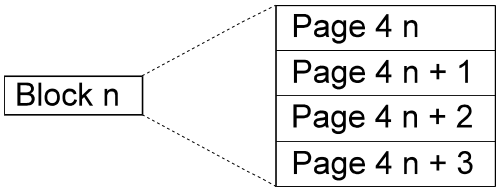
The table on the following page describes the memory configuration on the data carrier as delivered by Mikron:

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

Memory Mapping



Each block is devided into 4 pages.
One page consistis of 4 bytes.



Access to the memory is done page by page or block by block. See chapter 5.3.5. - 5.3.8.

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

Secret / Public: Access to an address in the secret area of the data carrier is only possible using cryptography and mutual authentication, access to the plain area is possible without cryptography (plain) and without authentication.

Block 0 defines the unique serial number (programmed during the production process and cannot be changed afterwards), the configuration page (configuration of the memory area) and the keys, Block 1 defines the logdata.

Blocks 4 to 7 can be used either as secret or public areas (configurable), and Blocks 2 to 7 either as read / write or read only areas (configurable). You can also modify keys and logdata and prevent them from being accessed.
Finally the configuration page itself can be set to read only.

It is extremely important to be particularly careful when using the configuration page (it can be set to read only once!), keys and logdata as you lose access to the secret area on the data carrier if you make a mistake.

For more details to the configuration page, keys and logdata see Chapter 5.

Attention: Changing of the Configuration page (page 1), Keys and Logdata must be done in secure environment. The data carrier must not be moved out of the communication field of the antenna during programming! We recommend to put the data carrier close to the antenna (zero-distance) and not to remove it during programming.

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

3. Serial Protocol and Command Set

3.1. Interface HITAG Read/Write Device ⇔ HOST

The device communicates with the host (processor, PC, ...) via serial interface using a baud rate of 9600 baud. Data transfer details are: 1 start bit, 8 data bits, 1 stop bit and no parity bit, Least Significant Byte is sent first.

3.1.1. General Definitions

The individual blocks show a common structure. Each block starts with the block length, followed by a block title (function number or status) and then the data. The data are transmitted transparently, i.e. you can use any character between 0x00 and 0xFF. Finally there is a check sum which is formed as EXOR - link of all transferred data.

General Data Transfer Format:

Byte	**1**	**2**	**3**	**4**	**.....**	**n**
Function	block length	block title / status	data	data	.....	check sum

Block length is the sum of all transferred bytes including block length but excluding check sum.
The check sum is calculated by bytes 1 to n-1.
Data bytes only are transmitted if data is transferred.

Transfer timeout intervals are defined as follows:

a) Character Delay

Character delay is the maximum time permitted to elapse between sending two consecutive characters of a block.

Character Delay ≤ 150 ms

b) Block Delay

There must be a minimum interval - defined as block delay - between two blocks sent, to allow for re-synchronization in case of malfunction.

Block Delay ≥ 160 ms

This block delay is only necessary if an error has occurred in the serial communication.

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

3.2. Command Set

The commands are divided into four groups:

1) HITAG - read and write commands (access to HITAG data carrier)
3) General commands (Reset command etc.)
4) Personalization commands (personalization of your read/write device)

3.2.1. HITAG - Read and Write Commands

These commands provide access to HITAG data carriers.

Command Name	Command Function
GetSnr	Reads the serial number of a data carrier
SelectSnr	Selects a data carrier ("prepares" it for a following read or write process)
SelectLast	Selects the last data carrier
HaltSelected	Sets the data carrier to Halt Mode ("mutes" a data carrier)
ReadPage	Reads a page (plain or cypher)
ReadBlock	Reads a block (plain or cypher)
WritePage	Writes a page (plain or cypher)
WriteBlock	Writes a block (plain or cypher)
TagAuthent	Executes single authentication
MutualAuthent	Executes mutual authentication
ReadAllPage	Reads a specific page (plain or cypher) of all data carriers

3.2.2. General Commands

These commands concern above all the read/write device, apart from the command ResetHFSystem, which also concerns the data carrier.

Command Name	Command Function
ResetSystem	Resets the system
ResetHFSystem	Turns off high frequency for 5 ms
SetBCD	Adapts the timing of the read/write device to the antenna
GetVersion	Reads the present software version and the serial number
EE_Read	Reads EEPROM data (memory on the read/write device)
EE_Write	Writes the EEPROM (memory on the read/write device)
ReadLRStatus	Reads the status of the antenna (malfunction indication)
SetPowerDown	Activates and deactivates the standby mode
SetOutput	Sets and resets the output pin for general purpose
ReadInput	Reads the input pin for general purpose

3.2.3. Personalization Commands

Use these commands to personalize your read/write device.

Command Name	Command Function
KeyInitMode	Starts the Personalization Mode
ReadControl	Reads the control bytes

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

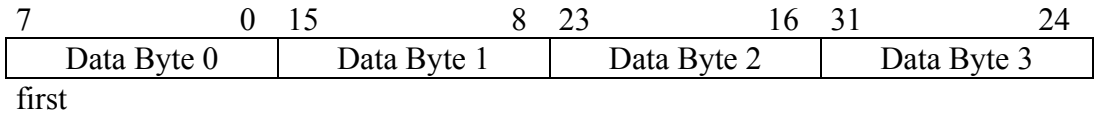
WriteControl	Writes the control bytes
ReadCryptoData	Reads keys, logdata or password from the EEPROM
WriteCryptoData	Writes keys, logdata or password into the EEPROM

3.3. Detailed Command Description

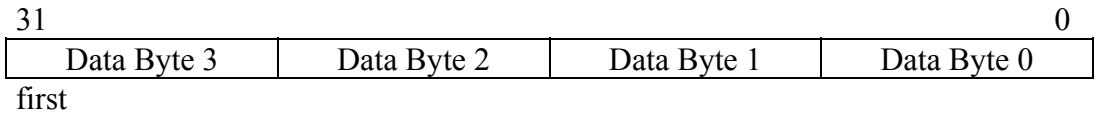
This section describes all the commands of the serial interface between read/write device and host.
You also find the function names of the Demo-C-Library here.

It is a characteristic of the Demo Library to store Data Bytes of lower order at lower addresses and receive or transmit them first via serial interface.

Serial Data:



Presentation by the Library:



Some errors can occur when executing a command on the read/write device. These errors are reported to the host with the answer to each command.
The resulting status information consists of one byte (signed char). If the command has been executed correctly, status (error-) information reads ZERO. An error is reported as a negative value.

The following error codes are defined:

Value	Description	Value	Description
0	no error	-9	CRYPTOBLOCK NOT INIT
-1	SERIAL error	-10	EEPROM error
-3	NOTAG error	-11	EEPROM - Wrong Old Data
-4	TIMEOUT error	-12	EEPROM - Write Protected
-7	AUTHENT error	-13	EEPROM - Read Protected
-8	ACKNOWLEDGEMENT error	-20	ANTENNA overload

Error Description

- SERIAL error: Error at the serial interface.
- NOTAG error: There is no data carrier within the communication field of the antenna.
- TIMEOUT error: There is not enough energy available to write on the data carrier.
- AUTHENT error: An error occured during the authentication process.
- ACKNOWLEDGEMENT error: The acknowledgement was not received correctly.
- CRYPTOBLOCK NOT INIT: A cryptographic command was transmitted without authentication.

The following error messages concern the read/write device:

- EEPROM error: EEPROM (of the read/write device) check sum error.
- EEPROM Wrong Old Data: On comparison old and new data prove inconsistent.
- EEPROM Write Protected: You attempted to write to the read/write device, although writing was not allowed.
- EEPROM Read Protected: You attempted to read to the read/write device, although reading was not allowed.
- ANTENNA overload: Broken or badly detuned antenna.

Bourgogne et Grasset — ZI Beaune Savigny –– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

3.3.1. GetSnr

This command provides the serial number of a data carrier.

Definition: *void proloc_GetSnr (DWORD *snr, char *more);*

Serial protocol:

HOST - Read/Write Device

0x02	'G'	0x45

Read/Write Device - HOST

	7 0	------	31 24		
0x07	Status	Data[0]	------	Data[3]	more	BCC

Note: *More* not equal zero (0) indicates that there is at least one additional data carrier in the reading area of the read/write device.

Status: 0 ... no error
- 1 ... SERIAL error
- 3 ... NOTAG

3.3.2. SelectSnr

This command selects the data carrier with the specified serial number *snr*. If there is no such data carrier in the field, a NOTAG error message is displayed.
In the case of errorfree execution the contents of page 1 (configuration) is saved in **otp*.

Attention: SelectSnr needs a preceding GetSnr. The serial number (snr) has to be the same as received with the preceding GetSnr (see Chapter 12.4, Examples).

Definition: *void proloc_SelectSnr (DWORD snr, DWORD *otp);*

Serial protocol:

HOST - Read/Write Device

	7 0	.....	.....	31 24	
0x06	'S'	snr	.....	.....	snr	BCC

Read/Write Device - HOST

	7 0	------	31 24	
n	Status	OTP-LSB	------	OTP-MSB	BCC

n = 2 if an error occured (error code in Status).
n = 6 if data were read from a data carrier (Status = 0).

Status: 0 ... no error
- 1 ... SERIAL error
- 3 ... NOTAG

3.3.3. SelectLast

Selects the data carrier with the ID that was read executing the last errorfree *proloc_GetSnr* command.
This command is an abbreviated version of *proloc_SelectSnr* as no serial number has to be transmitted via the serial interface and the contents of the OTP - Page is not returned.

Definition: *void proloc_SelectLast (void);*

Serial protocol:

HOST - Read/Write Device

0x02	'S'	0x51

Read/Write Device - HOST

0x02	Status	BCC

Status: 0 ... no error
- 1 ... SERIAL error
- 3 ... NOTAG

3.3.4. HaltSelected

Puts the selected data carrier into Halt Mode, which means that this data carrier remains silent until it leaves the high frequency field.
This allows you to identify also data carriers located farther away.

You can reset a data carrier previously turned off by HALT Mode using the command ResetHFSystem.

Definition: *void proloc_HaltSelected (void);*

Serial protocol:

HOST - Read/Write Device

0x02	'H'	0x4A

Read/Write Device - HOST

0x02	Status	BCC

Status: 0 ... no error
- 1 ... SERIAL error
- 8 ... ACKNOWLEDGEMENT error

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

3.3.5. ReadPage

Reads a page (4 bytes) on a selected data carrier. If no data carrier is selected, a NOTAG error will be generated.
Using the byte -*crypto*- you define whether you want to work in Encrypted Mode or not. Access to the secret area is only possible in Crypto Mode after a mutual authentication.
If -*crypto*- equals 1 (Crypto Mode) and you did not run an authentication procedure before, Status will be set to -9.

Definition: *void proloc_ReadPage (BYTE crypto, BYTE pagenr, char *data);*

Serial protocol:

HOST - Read/Write Device

0x04	'P'	crypto	pagenr	BCC

Read/Write Device - HOST

n	Status	Data[0]	.....	Data[3]	BCC

crypto: 1 ... crypto mode
0 ... plain mode

n = 2 if an error occured (error code in Status).
n = 6 if data were read from a data carrier (Status = 0).

Status: 0 ... no error
- 1 ... SERIAL error
- 3 ... NOTAG
- 9 ... CRYPTOBLOCK NOT INIT

3.3.6. ReadBlock

Reads a block (16 bytes) on the selected data carrier.
The start address is specified by pagenr. Data is read from the start address until the end of the corresponding block. Thus a datalength of 4, 8, 12 or 16 bytes is possible.

Use byte *-crypto-* to define whether you want to work in Encrypted Mode or not. Access to the secret area is only possible in Crypto Mode after a mutual authentication.
If *-crypto-* equals 1 (Crypto Mode) and you did not run an authentication procedure before, Status will be set to -9.

Definition: *void proloc_ReadBlock (BYTE crypto, BYTE pagenr, char *data);*

Serial protocol:

HOST - Read/Write Device

0x04	'B'	crypto	pagenr	BCC

Read/Write Device - HOST

n+2	Status	Data[0]	.....	Data[n]	BCC

n = 2 if an error occured (error code in Status).
n = 6, 10, 14, 18 depending on the page address.

Status: 0 ... no error
- 1 ... SERIAL error
- 3 ... NOTAG
- 9 ... CRYPTOBLOCK NOT INIT

Bourgogne et Grasset — ZI Beaune Savigny — 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

3.3.7. WritePage

Writes a page (4 bytes) onto the selected data carrier.
If no data carrier is selected, a NOTAG error will be generated.

Use byte *-crypto-* to define whether you want to work in Encrypted Mode or not. Access to the secret area is only possible in Crypto Mode after a mutual authentication.
If *-crypto-* equals 1 (Crypto Mode) and you did not run an authentication process before, Status will be set to -9.

Definition: *void proloc_WritePage (BYTE crypto, BYTE pagenr, char *data);*

Serial protocol:

HOST - Read/Write Device

0x08	'p'	crypto	pagenr	Data[0]	.....	Data[3]	BCC

Read/Write Device - HOST

0x02	Status	BCC

Note: To substantially increase the data reliability we strictly recommend to read the previously written data (read after write).

Status: 0 ... no error
- 1 ... SERIAL error
- 3 ... NOTAG
- 9 ... CRYPTOBLOCK NOT INIT

3.3.8. WriteBlock

Writes a block (16 bytes) of the selected data carrier.
If you did not select any data carrier, a NOTAG error will be generated.

The start address is specified by pagenr. Data is written from the start address until the end of the corresponding block.

Use byte *-crypto-* to define whether you want to work in Encrypted Mode or not. Access to the secret area only is possible in Crypto Mode after a mutual authentication.
If *-crypto-* equals 1 (Crypto Mode) and you did not run an authentication procedure before, Status will be set to -9.

Definition: *void proloc_WriteBlock (BYTE crypto, BYTE pagenr, char *data);*

Serial protocol:

HOST - Read/Write Device

n+4	'b'	crypto	pagenr	Data[0]	.....	Data[n]	BCC

Read/Write Device - HOST

0x02	Status	BCC

Note: To substantially increase the data reliability we strictly recommend to read the previously written data (read after write).

Status: 0 ... no error
- 1 ... SERIAL error
- 3 ... NOTAG
- 9 ... CRYPTOBLOCK NOT INIT

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

3.3.9. TagAuthent

Carries out the single authentication procedure (authentication of the data carrier). The authentication procedure is aborted after sending the data carrier logdata. After this abbreviated authentication procedure the data carrier can only be accessed using *GetSnr* or the command *ResetHFSystem*.
You cannot use any Crypto commands!

Using -*loginfo*- you can chose between Log information (Keys and Logdata) A and B.

Definition: *void proloc_TagAuthent (BYTE loginfo);*

Serial protocol:

HOST - Read/Write Device

0x03	'a'	loginfo	BCC

Read/Write Device - HOST

0x02	Status	BCC

loginfo: 0 ... loginfo A
1 ... loginfo B

Status: 0 ... no error
- 1 ... SERIAL error
- 7 ... AUTHENT error

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

3.3.10. MutualAuthent

Carries out the full authentication procedure of the data carrier and the read/write device.
After this mutual authentication you are allowed to edit areas which can only be accessed in SECRET Mode.
Use a Plain command (that is encrypted), *ResetHFSystem* or *GetSnr* to exit this mode.
Using -*loginfo*- you can choose between Log information (Keys and Logdata) A and B.

Definition: *void proloc_MutualAuthent (BYTE loginfo);*

Serial protocol:

HOST - Read/Write Device

0x03	'A'	loginfo	BCC

Read/Write Device - HOST

0x02	Status	BCC

loginfo: 0 ... loginfo A
1 ... loginfo B

Status: 0 ... no error
- 1 ... SERIAL error
- 7 ... AUTHENT error

3.3.11. ReadAllPage

Reads all Pages of Data Carriers in the active antenna field.

Definition: *void proloc_ReadAllPage (BYTE pagenr, BYTE mode, BYTE *data, BYTE *datalen);*

Serial protocol:

HOST - CORE MODULE

0x04	0x98	mode	pagenr	BCC

mode: Bit 0: 0=use KEY0 for Authentification
1=use KEY1 for Authentification
Bit 1: 0=Plain (without Authentification)
1=Crypto (with Authentification)

CORE MODULE - HOST

n+2	Status	Data[0]	.....	Data[3]	BCC

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

3.3.12. ReadAllSnr A

Reads all Serial numbers of Data Carriers in the active antenna field. This command is also called the fast command A.

Serial protocol:

HOST - CORE MODULE

0x02	0x9B	BCC

Read/Write Device – HOST

Data[0]	.....	Data[n+1]

For every tag present you should receive 7 bytes from the reader:

0x06	Status	Snr	snr	snr	snr	BCC

When no more tags are found you receive 5 bytes from the reader:

0x04	Status	Collisions[0]	Collisions[1]	BCC

Status – Equal to 0 if command completed with no error, to –3 if no tag was found or some other error code if at least one tag was found but the command stopped because of an error during execution.
False Collisions - Can be caused by detuned antennas or electromagnetic influences. Their effect is mainly to increase the read time. Including this information in the response helps in adjusting the external environment.

3.3.13. ReadAllSnr B

Reads all Serial numbers of Data Carriers in the active antenna field. This command is also called the fast command B.

Serial protocol:

HOST - CORE MODULE

0x03	0x9C	Block Flag/Page Number	BCC

Block Flag/Page Number – Bits 0-6 indicate the page address. Bit 7 is set to 0 for page access, to 1 for block access. In case that no page or block retrieval is desired, this byte should be set to 0.

Read/Write Device – HOST

Data[0]	.....	Data[n+1]

For each tag found the following frame is sent:

NBytes	Status	Iter	snr[0]	snr[1]	snr[2]	snr[3]	otp[0]	otp[1]	otp[2]	otp[3]	Opt Data	BCC

NBytes – Number of bytes in the frame following the start byte.

Status – If equal to 0, no error occurred. If bit 0 is set, an error occurred during trying to select the tag; it is possible that the serial number does not correspond to a real tag or that the retrieved configuration page is not correct. If bit 1 is set, an error occurred during page/block access; it is possible that the retrieved data is not correct. If bit 2 is set, an error occurred while trying to put the tag into halt mode; it is possible that the tag is not halted.

Iter – The number of the current iteration. First iteration has number 0. The execution of the command is stopped by the reader after 255 iterations. This field is provided so that the host can decide whether the command is worth to be continued, as an increased number of iterations is a mark of difficult electromagnetic conditions.

snr – Tag serial number.

otp – Tag configuration page.

Optional Data – If no page/block read has been required, this field is absent. For page read this field is 4 bytes long and contains the page data. For block read this field is 1, 2, 3 or 4 bytes long (depending on the page address) and contains the block data.

When no more tags are found or some error occurred the frame below is sent, which marks the end of the reader response:

0x04	Status	False Collisions[0]	False Collisions[1]	BCC

See ReadAllSnr A command for explanation of the fields.

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

3.3.14. ResetSystem

This command comprises several functions. Firstly, it helps to establish errorfree communication of the serial interface, secondly, this command resets the complete processor system.

Definition: *void proloc_Reset (void);*

Serial protocol:

HOST - Read/Write Device

0x02	'R'	0x50

Read/Write Device - HOST

0x02	Status	BCC

Status: 0 ... no error
- 1 ... SERIAL error

3.3.15. ResetHFSystem

This function turns off the HF-part of the module for about 40 ms. This means that all data carriers are reset and data carriers that were in HALT Mode will respond again.

Definition: *void proloc_HFReset (void);*

Serial protocol:

HOST - Read/Write Device

0x02	'h'	0x6A

Read/Write Device - HOST

0x02	Status	BCC

3.3.16. SetBCD

This command (SetBitClockDelay) adjusts the timing of the read/write device to the antenna. The command has to be operated once, when an antenna and a read/write device are assembled the first time and the system start-up is done. If the antenna is changed in an installed system the command has to be operated again, to adjust the timing of the read/write device to the new antenna. See Chapter 8 "Tuning of the antenna phase".

Definition: *void proloc_SetBCD (char bitclockdata);*

Serial protocol:

HOST - Read/Write Device

0x03	'F'	bitclockdata	BCC

bitclockdata: LSB

bitclockdelay Bit 3	bitclockdelay Bit 2	bitclockdelay Bit 1	bitclockdelay Bit 0	0	0	0	0

bitclockdelay: 0 ... 15_{dec} possible

Read/Write Device - HOST

0x02	Status	BCC

Status: 0 ... no error
- 1 ... SERIAL error
- 8 ... ACKNOWLEDGEMENT error

Bourgogne et Grasset — ZI Beaune Savigny — 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

3.3.17. GetVersion

This command retrieves the serial number of the station, the version number of the processor software and its date of creation.

Definition: *void proloc_GetVersion (char *data);*

Serial protocol:

HOST - Read/Write Device

0x02	'V'	0x54

Read/Write Device - HOST

0x1D	Status	data[0]	.....	data[26]	BCC

data[0].....data[7] Version (format: X.YY.ZZZ)
data[8].....data[15] Date (format: DD.MM.YY)
data[16]....data[26] Serial number (11 characters)

Status: 0 ... no error
- 1 ... SERIAL error

3.3.18. EE_Read

Reads - starting with the chosen address - up to 16 data bytes from the user memory in the EEPROM of the read/write device. If you reach the limit of the address area the read/write command is finished.

$0 \leq addr \leq 84$, $nmb \leq 16$

Definition: *void proloc_ReadEEData (char addr, char nmb, char *data);*

Serial protocol:

HOST - Read/Write Device

0x04	'E'	addr	nmb	BCC

Read/Write Device - HOST

n + 2	status	data[0]	.....	data[n]	BCC

Status: 0 ... no error
- 1 ... SERIAL error
- 10 ... EEPROM error

3.3.19. EE_Write

Writes - starting with the chosen address - up to 16 data bytes into the user memory of the EEPROM of the read/write device. If you reach the limit of the address area the read/write command is finished.

$0 \leq addr \leq 84$, $nmb \leq 16$

Definition: *void proloc_WriteEEData (char addr, char nmb, char *data);*

Serial protocol:

HOST - Read/Write Device

0x02	'e'	addr	nmb	data[0]	.....	data[n]	BCC

Read/Write Device - HOST

2	status	BCC

Status: 0 ... no error
- 1 ... SERIAL error
- 10 ... EEPROM error

3.3.20. ReadLRStatus

Reads the antenna overload bit. In case of broken or badly detuned antenna the overload bit is high.

Definition: *proloc_ReadLRStatus (void);*

HOST - Read/Write Device

0x02	'r'	0x70

Read/Write Device - HOST

0x02	Status	BCC

Status: 0 ... no error
- 1 ... SERIAL error
- 20 ... ANTENNA overload

3.3.21. SetPowerDown

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

To turn the read/write device into standby mode the onoff bit is set to zero. To activate the amplifier again this bit must be set (by default the read/write device is in standby mode).

Definition: *proloc_SetPowerDown (char onoff)*

HOST - Read/Write Device

0x03	'D'	onoff	BCC

onoff = 0 ... Standby-Mode is inactive

Read/Write Device - HOST

0x02	Status	BCC

Status: 0 ... no error
- 1 ... SERIAL error

3.3.22. SetOutput

By default one portpin of the processor is defined as output. You can set (5 V) or reset (0 V) this output using the command *SetOutput*. The output is buffered by an inverting CMOS driver.

Definition: *void proloc_SetOutput (BYTE port);*

Serial protocol:

HOST - Read/Write Device

0x02	'O'	port	BCC

with:

7	6	5	4	3	2	1	0
x	x	x	x	x	x	x	Out1

1 ... reset (0 V)
0 ... set (5 V)

Read/Write Device - HOST

0x02	Status	BCC

Status: 0 ... no error
- 1 ... SERIAL error

3.3.23. ReadInput

By default one portpin of the processor is defined as input. You can inquire the status of this pin using the command ReadInput. The input is buffered by an inverting schmitt trigger input driver. **(ATTENTION: Pins are internally pulled up!).**

Definition: *void proloc_ReadInput (BYTE *input);*

Serial protocol:

HOST - Read/Write Device

0x02	'I'	0x4B

Read/Write Device - HOST

0x03	Status	input	BCC

with:

7	6	5	4	3	2	1	0
x	x	x	x	x	x	x	In1

1 ... reset (0 V)
0 ... set (5 V)

Status: 0 ... no error
- 1 ... SERIAL error

3.3.24. WritePorts

This Output pins P0.0-P0.6 can be set or reset by using the command WritePorts. The joutput is buffered by an inverting CMOS driver.

Definition: *void proloc_WritePort0 (BYTE data, BYTE mode);*

Serial protocol:

HOST - CORE MODULE

0x04	'o'	data	mode	BCC

data:

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

mode:

=0: The bits in data are directly written to the output-configurated portpins

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

=1: The actual status of the output-configurated portpins is AND-combined with the bits in data. The result is written to the output-configurated portpins
=2: The actual status of the output-configurated portpins is OR-combined with the bits in data. The result is written to the output-configurated portpins
=3:The actual status of the output-configurated portpins is EXOR-combined with the bits in data. The result is written to the output-configurated portpins

CORE MODULE - HOST

0x02	Status	BCC

Status: 0 ... no error
- 1 ... SERIAL error

3.3.25. GetDspVersion

This command retrieves the version number of the DSP-software.

Definition: *void proloc_GetVersion (char *data);*

Serial protocol:

HOST - CORE MODULE

0x02	'v'	0x54

CORE MODULE - HOST

0x1C	Status	data[0]	.....	data[7]	BCC

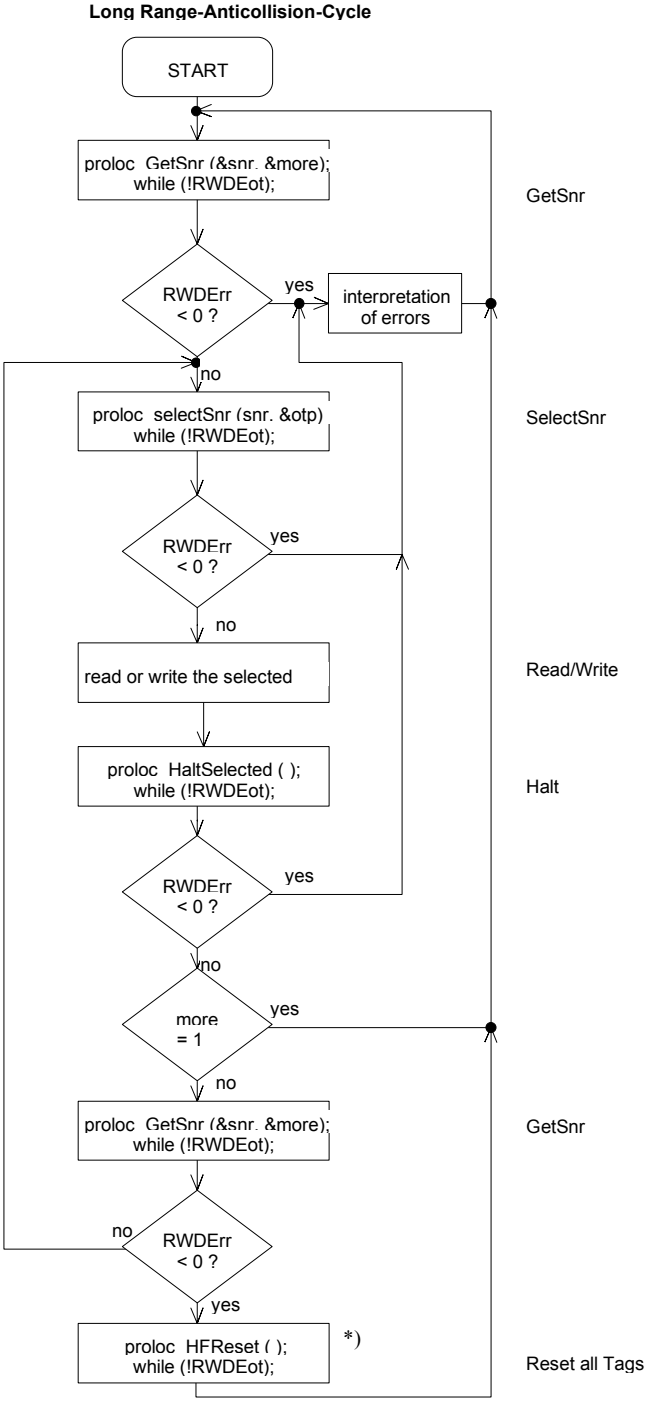
data[0].....data[7] Version (format: ASCII)

3.4. Examples

In the following please find examples of read/write cycles both for plain and encrypted access in order to illustrate the command sequence.

3.4.1. Anticollision Cycle

In case of several data carriers in the reading area of the read/write device the GetSnr command indicates this by the *more* byte. To select one of these data carriers for following read or write operations an anticollision cycle must be executed as described in the following flow chart.



*) In case you want to access the same tags for several times.

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

3.4.2. READ PLAIN

GetSnr	Reads the serial number of a data carrier in the communication field of the antenna
SelectSnr	Selects (prepares) the data carrier for a following read process.
Read	Reads a data carrier
HaltSelected	Mutes the just treated data carrier

3.4.3. WRITE PLAIN

GetSnr	
SelectSnr	
Write	Writes data to a data carrier
HaltSelected	Mutes the just treated data carrier

3.4.4. READ CRYPTO

GetSnr	
SelectSnr	
MutualAuthent	Carries out the mutual authentication of the data carrier and the read/write device.
Read (Crypto)	
HaltSelected	

Bourgogne et Grasset –– ZI Beaune Savigny –– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

3.4.5. WRITE CRYPTO

GetSnr

SelectSnr

MutualAuthent

Write (Crypto)

HaltSelected

Note: If you want to read the serial number once again after having transmitted the command Select, you should do this by reading Page 0. In case you want to read the serial number with the command GetSnr, you have to transmit the command GetSnr twice as the mode is switched.

To substantially increase the data reliability we strictly recommend to read the previously written data (read after write).

When using the C-Library for programming please read the Appendix (Headerfile Listing) for detailed information.

3.5. Commands for Configuration and Personalization of the Read/Write Device

This group of commands deals with a special area of the read/write device EEPROM. Some security features are provided in order to avoid forbidden or unintentional execution of these commands.

- The commands are available only if the read/write device is in a special mode (Key-Init Mode).
- To enter the Key-Init Mode a password is needed.
- The checksum in the serial protocol differs form the one used for other commands (BCC).
- In order to change data in the EEPROM the user has to know the old values.

For further information please see Chapter 5 (Personalization).

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

3.5.1. KeyInitMode

With this command the read/write device is set to KeyInitMode.

Definition: *proloc_KeyInitMode (unsigned long password)*

HOST - Read/Write Device

		7 0	15 8	23 16	31 24	
0x06	'K'	PW0	PW1	PW2	PW3	BCC

Read/Write Device - HOST

0x02	Status	BCC

PW0 ... PW3 ... password
BCC ... Standard_BCC calculation formed as EXOR-link of all transferred data

Status: ... 0 ... no error
- 1 ... SERIAL error
- 11 ... EEPROM error. The password was incorrect.
The HITAG read/write device remains in normal operating mode.

The password (🕒 Logdata ensures that none but authorized persons are able to enter the KeyInitMode.

Attention: After the successful execution of this command the BCC calculation changes. From now on BCC is build as a 8-bit sum without carry.

The read/write device changes BCC-calculation automatically. On the host system the user is responsible for the new BCC-calculation.
The library prolib5 provides the function proloc_SetBCCMode ( ). See Appendix.

Exit of KeyInitMode is done by the command ResetSystem or by a failing WriteCryptoData.

3.5.2. ReadCryptoData

This command reads a data package (4 data bytes) of the HITAG - VEGAS read/write device. Access rights are verified automatically by the HITAG-VEGAS read/write device before this command is executed. (The read/write device checks if the memory has been locked or not).

Definition: *proloc_Read EEPROM (char com, unsigned long *data)*

HOST - Read/Write Device

0x03	'X'	Com	BCC

Read/Write Device - HOST

		7 0	15 8	23 16	31 24	
0x05	Status	D0	D1	D2	D3	BCC

Com ... defines which information is to be read
BCC ... 8-bit sum without carry

Status: 0 ... no error
- 1 ... SERIAL error or Read/Write Device is not in KeyInitMode
- 13 ... EEPROM read protected.
The HITAG read/write device remains in Key_Init Mode.

3.5.3. WriteCryptoData

This command writes a data package (4 data bytes) to the HITAG read/write device. This command requires the old data to be transmitted as well, which means that data can only be changed if the user knows the old written data.

Definition: *proloc_Write EEPROM (char com, unsigned long old, unsigned long new)*

HOST - Read/Write Device

0xB	'Y'	Com	OD0	OD1	OD2	OD3	ND0	ND1	ND2	ND3	BCC

Read/Write Device - HOST

0x02	Status	BCC

Com ... defines which information is to be read
OD0 ... OD3 ... old data
ND0 ... ND3 ... new data
BCC ... 8-bit sum without carry

Status: 0 ... no error
- 1 ... SERIAL error or Read/Write Device is not in KeyInitMode
- 11 ... EEPROM Wrong Old Data
- 12 ... EEPROM read protected.

If any error occurs, KeyInitMode is exited immediately.

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

3.5.4. ReadControl

With this command you read **both** control bytes of the read/write device.

Definition: *proloc_ReadControl (char *control_bytes)*

HOST - Read/Write Device

0x02	'C'	BCC

Read/Write Device - HOST

0x04	Status	C_RW	C_WO	BCC

BCC ... 8-bit sum without carry
C_RW ... Control_RW (see chapter 3.5.7
C_WO ... Control_WO Control Bytes Function)

Status: 0 ... no error
- 1 ... SERIAl error or Read/Write Device is not in KeyInitMode

3.5.5. WriteControl

Writes **both** control bytes in the read/write device. An attempt to change a bit from 0 to 1 has no effect.

Definition: *proloc_WriteControl (char *CONTROL_RW, char CONTROL_WO)*

HOST - Read/Write Device

0x04	'c'	C_RW	C_WO	BCC

Read/Write Device - HOST

0x02	Status	BCC

C_RW ... Control_RW (see chapter 12.5.7
C_WO ... Control_WO Control Bytes Function)
BCC ... 8-bit sum without carry

Status: 0 ... no error
- 1 ... SERIAL error or Read/Write Device is not in KeyInitMode

3.5.6. List of Commands

Command		Function
'C'		Read Control_RW, Control_WO
'c'		Write Control_RW, Control_WO
'X' '0'		Read Password
'X' '1'		Read Key A
'X' '2'		Read Key B
'X' '3'		Read Logdata 0A
'X' '4'		Read Logdata 0B
'X' '5'		Read Logdata 1A
'X' '6'		Read Logdata 1B
'Y' '0'		Write Password
'Y' '1'		Write Key A
'Y' '2'		Write Key B
'Y' '3'		Write Logdata 0A
'Y' '4'		Write Logdata 0B
'Y' '5'		Write Logdata 1A
'Y' '6'		Write Logdata 1B

3.5.7. Control Bytes Function

Use the two control bytes to activate the various security levels. You can lock every single information using the corresponding bits.

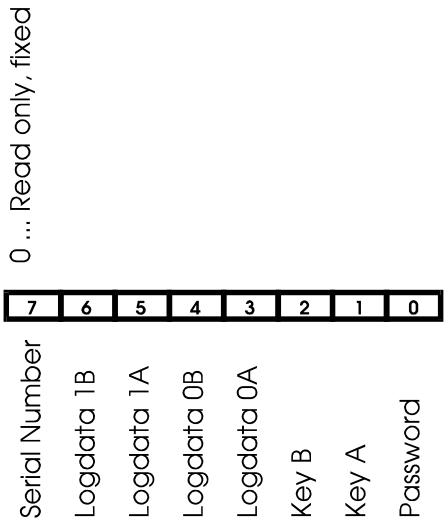
If you have already set a bit to ZERO, it cannot be changed back to ONE again. Once a security level has been assigned, it becomes irreversible.

This information is always tested before accessing a variable. If access is not permitted and you transmit a read command, the data is set to 0, an attempt to write is not carried out, and you quit Key-Init Mode. (See Chapter 3.5.3 WriteCryptoData)

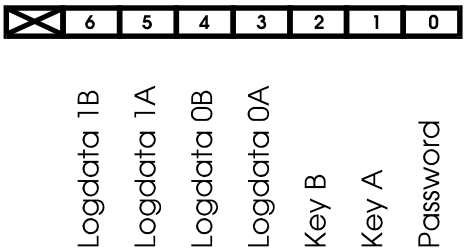
Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

Byte 1 (Control_RW) controls reading access to the data bytes, Byte 2 (Control_WO) controls writing access.

Control_RW:



Control_WO:



On delivery all HITAG VEGAS read/write device bits (Control_RW and Control_WO) are set to 1, except Bit 7 of CONTROL_RW (serial number). Resetting the bits allows you to realize the following configurations:

CONTROL_WO	CONTROL_RW	Function
1	1	read and write
1	0	write only
0	X	neither read nor write

ATTENTION: You cannot change bits that have been set to 0 after transmitting the command!

4. Security Considerations

Developing the HITAG VEGAS System special consideration was given to aspects of security. The following items represent the fundamental framework of the security concept:

- cryptography
- mutual authentication
- password verification
- cyclic redundancy check

4.1. Operating Security

The following mechanisms guarantee the operation security of the HITAG VEGAS system.

4.1.1. Antenna Short Circuit

The HITAG VEGAS read/write device does not get permanently damaged in case of a brief antenna short circuit.

4.2. Data Reliability

All the commands and data transferred from the read/write device to the data carrier are secured by Cyclic Redundancy Check.

Note: To avoid problems caused by insufficient energy transmitted to the tag or by electromagnetic disturbances we recommend to read data twice (double-read).

4.2.1. CRC of a Data Stream between Read/Write Device and Data Carrier

Every data stream sent (commands, addresses, user data) is first checked for data errors by a data carrier-integrated 8-bit CRC generator and then executed. Normally the data carrier responds to each data stream from the read/write device with an acknowledgement signal or with a data block.
The CRC is formed over commands and addresses or the plain data respectively and in the case of Encrypted Mode it is also encrypted.

The generator polynomial of the data carrier CRC generator reads:

$$u8 + u4 + u3 + u2 + 1 \text{ ..... } = 1\ D$$

and the CRC preassignment is: FF

4.2.2. Checking User Data

(this check is carried out in the HITAG VEGAS read/write device)

Security of the data read from the data carrier by the HITAG VEGAS read/write device remains with the user for reasons of flexibility. Therefore, you can choose flexible check sums and store them in the EEPROM together with the data. You can protect sensitive data better than less sensitive data, thus permitting optimized operation times.

Detailed instructions how to use and calculate Cyclic Redundancy Check (CRC) are available at Mikron in a document named: *HITAG VEGAS - Contactless Data Transmission, Data Reliability and Integrity*.

4.3. Data Privacy

The use of cryptography (Stream Cypher), mutual authentication, and password verification prevents any possibility of monitoring and copying the data channel. This guarantees highest possible data security in the secret area of the data carrier.
To make use of cryptography you need secret data: keys and logdata.

> **Keys** are used to **initialize the crypto block**
> and **logdata** are used for **mutual authentication**.

The data carriers and the *HITAG VEGAS* read/write device are provided with identical transport keys and transport logdata ex Mikron so that you can start operating them right away.

In order to offer our OEM clients high flexibility, the configuration of the data carrier memory, password, keys and logdata can be changed. (See Chapter 14, Personalization).

We strictly recommend to rigorously restrict these possibilities for the end customers (by setting the configuration page to read only, setting password, keys and logdata to neither read nor write).

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

5. Personalization

In order to profit from the full functionality of the *HITAG VEGAS* data carrier, the read/write device has to support the data carrier´s cryptographic feature.

This requires the use of some secret data (keys, logdata). The process of **loading these data** into the **HITAG VEGAS read/write device** is called **personalization**. The analogous **personalization** procedure has to be carried out on your **data carrier**. The read/write device and the data carriers are prepersonalized by Philips by means of defined Transport Keys and Transport Logdata. Therefore you can use the HITAG VEGAS read/write device without changing any data. Because of security considerations we recommend to use own keys and logdata. So only persons who got the authorization from you are able to access the secret area of the data carrier. To use own keys and logdata you have to personalize read/write device and data carrier. This process is described in the following chapters.

Make sure you are in safe environment while writing these secret data to the data carrier or the HITAG VEGAS read/write device. This prevents possible listening into the communication between HOST and read/write device.

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

5.1. General Definitions

In order to be able to read data from the secret area of a data carrier, you have to carry out a procedure called authentication. To do this you need special data (keys and logdata).
The authentication is automatically carried out by the HITAG VEGAS read/write device.

14.1.1. Definition of the Keys

Keys are cryptographic codes, which determine data encryption during data transfer between HITAG VEGAS read/write device and data carrier.
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 HITAG VEGAS read/write device and on the data carrier is sufficient.

The keys are predefined by Mikron by means of defined Transport Keys (both keys show the same bit map). They can be written to, which means that they can be changed.
It is impossible to read the keys as you can see in the memory mapping page 6.

5.1.1. Definition of the Logdata

Logdata represent "passwords" needed to gain access to secret areas on the data carrier. 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 data carrier and the read/write device.

ad Key A:	Logdata 0 A	"Password" which the data carrier 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 data carrier 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). HITAG VEGAS read/write device and data carrier are configured in a way that the logdata 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 HITAG VEGAS read/write device and on the data carrier!

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

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

on the HITAG read/write device		on the data carrier	
KEY A	⇔	KEY A	⎫
LOGDATA 0A	⇔	LOGDATA 0A	⎬ Set A
LOGDATA 1A	⇔	LOGDATA 1A	⎭
KEY B	⇔	KEY B	⎫
LOGDATA 0B	⇔	LOGDATA 0B	⎬ Set B
LOGDATA 1B	⇔	LOGDATA 1B	⎭

Attention: Keys and logdata only can be changed if the Transport Key and the Transport Logdata are known respectively the already changed values (´old values`)!

Communication of Transport Keys and Transport Logdata is done separately from the HITAG VEGAS read/write device Description.

5.2. Personalization Conception

To guarantee utmost security and flexibility Mikron worked out a personalization conception that shall be shortly described in the following:

The first stage is a test that is done by the producer respectively Mikron. Here the serial number is fixed (the serial number cannot be changed any more) and Transport Keys and Transport Logdata are preprogrammed in the data carrier and the HITAG VEGAS read/write device.
In the next stage the OEM customer or the System House program their own keys and logdata fix read only data and configure the memory of the data carrier. We recommend to lock sensitive areas, that means for example to prevent the possibility to change keys and logdata for the end user.
In the last stage the user just reads and writes the memory of the data carrier.

5.3. Configuration of the HITAG VEGAS Data Carrier

You have the possibility to configure parts of the memory area of the data carrier according to your needs (see also Chapter 5). You realize this configuration in the configuration page. This is where you also define whether keys and logdata (personalization of the data carriers) can be changed or not.

5.3.1. Organizing the Configuration Page

The configuration page (in the following called OTP page) consists of 4 bytes, the first two bytes are used, the other two bytes can be used by the system integrator.

Configuration Page

OTP 0	OTP 1		

(See memory mapping on page 6).

The bitmaps in OTP bytes 0 and 1 (bytes of the configuration page) determine the configuration of the memory, i.e. they define which area is secret or public, r/w, ro, wo or neither read nor write.

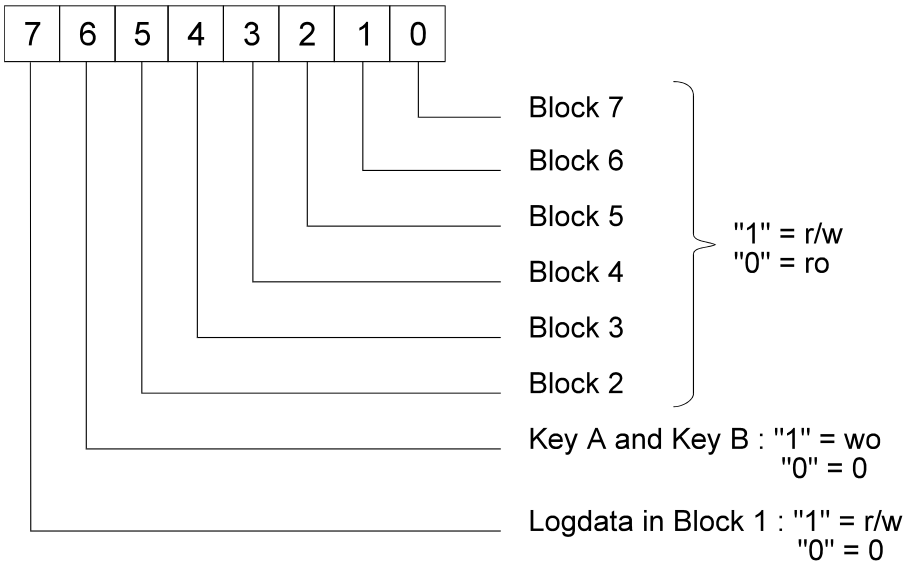
You can allocate and write the OTP bytes freely until the configuration page is locked (OTP Byte 1, Bit 4 is set to ”0”).
After that these bytes are read only bytes and the configuration of the data carrier memory cannot be changed any more.

Attention: Once set to ro the configuration page (OTP - Bytes) cannot be changed back to r/w again (data carrier is hardware protected)!

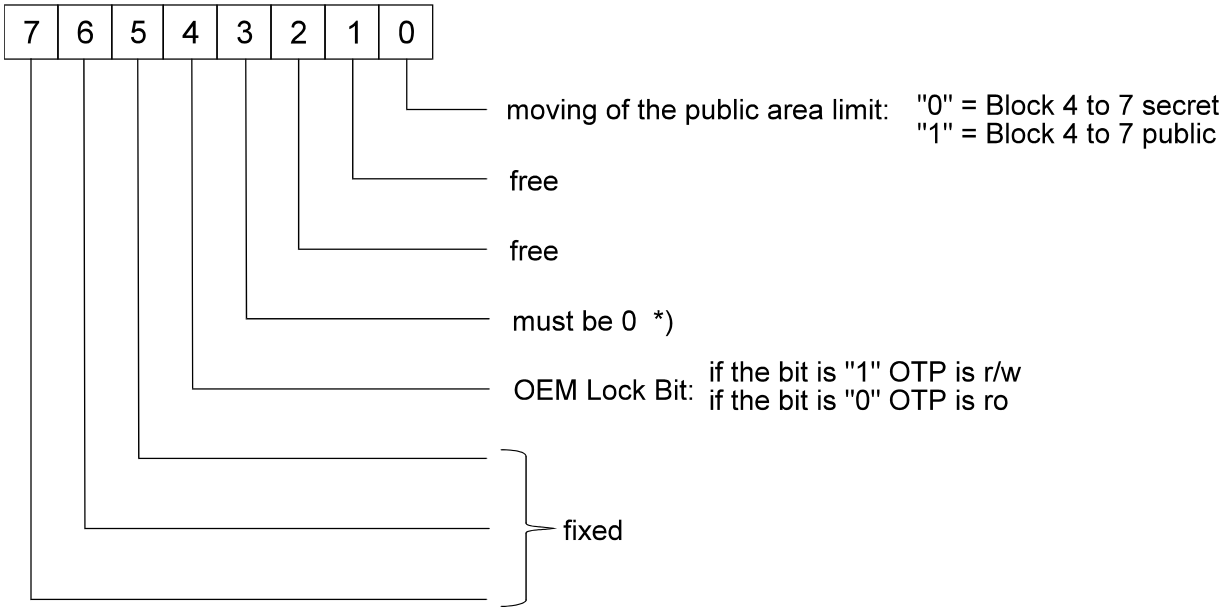
Explanations of abbreviations used:

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

5.3.2. OTP-Byte 0



5.3.3. OTP-Byte 1



As soon as the OEM Lock Bit is set to 0 the configuration page cannot be changed any more!

***) Changing this bit the data carrier cannot be operated any more!**

5.3.4. Default Configuration of HITAG VEGAS Data Carriers

HITAG VEGAS data carriers are delivered with the following configuration by Mikron:

Serial Number:	Read Only	-	fixed
Key A, Key B:	Write Only	-	can be changed
Logdata:	Read/Write	-	can be changed
OTP Page:	Read/Write	-	can be changed
Blocks 2 - 7:	Read/Write	-	can be changed
Blocks 4 - 7:	Public Access	-	can be changed

According to that the OTP bytes display the pattern illustrated below:

OTP Byte 0

Bit 7							Bit 0
1	1	1	1	1	1	1	1

OTP Byte 1

Bit 7							Bit 0
0	0	1	1	0	1	1	1

You cannot change Bits 5, 6, and 7 of OTP Byte 1 (gray background). If you attempt to write the configuration page with a bitmap that changes one of these three bits, the Write command will be executed without displaying an error message but the memory contents of OTP 1/Bit 5, OTP 1/Bit 6, OTP 1/Bit 7 will remain unchanged.

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

It has already been mentioned that the memory configuration is determined by the bitmap in OTP Bytes 0 and 1. You can change this bitmap until you set the OEM Lock Bit for the configuration page (OTP 1/Bit 4) to ”0”. This process is irreversible, which means that this bit locks the configuration page itself so that you cannot gain write-access to the 4 OTP bytes any more. This feature protects the data carrier from accidental changes of the configuration or manipulation by unauthorized persons.

Recommendation: Before delivering data carriers to end users, the configuration page should be set to read only (OTP 1/Bit 4 = ”0”) in any case!

5.3.5. Description of the Individual Configuration Options

Logdata - OTP 0 / Bit 7

If you set Bit 7 (OTP 0) to "0", the logdata on the data carrier cannot be changed again!

Key A and Key B - OTP 0 / Bit 6

You can change the keys until you set the OTP 0 / Bit 6 to ”0”. After that you cannot access Pages 2 and 3 any longer, the keys can be neither read nor changed.

Attention: If neither Key A nor Key B of the data carrier and the HITAG VEGAS read/write device are identical, you cannot access the secret area on that data carrier! Access to the plain area of the data carrier (e.g. serial number) is possible in any case.

Memory configuration for Blocks 2 ... 7 - OTP 0 / Bits 0 ... 5

If the OTP bit reads ”1”, the corresponding block can be read and written. If the bit is set to ”0”, the corresponding block can only be read. It does not matter whether the block is located in the secret or the public area of the data carrier.

You can choose any bit map you like, such as:

OTP 0/	Bit 0	”1”	Block 7	read and write
	Bit 1	”0”	Block 6	read only
	Bit 2	”0”	Block 5	read only
	Bit 3	”1”	Block 4	read and write
	Bit 4	”0”	Block 3	read only
	Bit 5	”1”	Block 2	read and write

Within one block the configuration is always identical, that means either all 4 pages are read/write or all of them are read only.

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

OTP 1 / Bit 5, 6 and 7

These three bits cannot be changed.

OTP 1 / Bit 4

Is this bit set to "0" the configuration page only can be read, so the configuration of the data carrier can not be changed again!

Attention: Once the OEM Lock Bit is set to zero, the memory configuration cannot be changed again. This process is irreversible !

OTP 1 / Bit 3

You must not change this bit to ”1”, it must be "0" or the data carrier cannot be operated any more!

OTP 1 / Bits 1 and 2

You can use these two bits whichever way you like as they are of no consequence for the data carrier configuration.

Moving the Public area limit: OTP 1 / Bit 0

This bit determines the access type for Blocks 4 to 7:

OTP 1 / Bit 0 =	”0”	Access to Blocks 4 to 7	SECRET
OTP 1 / Bit 0 =	”1”	Access to Blocks 4 to 7	PUBLIC

You can choose the type of access only for the total of Blocks 4 to 7.

OTP Bytes 2 and 3

You can use these two bytes freely. They will not affect memory configuration. For example, the OEM client can put his own OEM serial number here.

Attention: These two bytes, too, are set to read only by the OEM Lock Bit (OTP 1 / Bit 4 = ”0”)!

Bourgogne et Grasset — ZI Beaune Savigny –– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

5.4. Changing Keys and Logdata

You do not have to change keys and logdata in order to operate a system with the read/write device because access to the secret area of the data carrier is possible with the Transport Keys and Transport Logdata. Nevertheless we strictly recommend to change these data in order to avoid unauthorized access to the secret area of the data carrier.

If you change keys and logdata, you have to place the data carrier directly on the antenna or hold it directly to it (0-distance)! In order to avoid any errors do not move the data carrier during this write process and be sure that you are in a safe environment without electrical noise.

5.4.1. Changing Keys

Please, note the order of the steps!

1. Access the data carrier (using the Transport Keys).
2. Change one key (e.g.: Key A) on the data carrier, i.e., overwrite the corresponding page on the data carrier (in this case page 2) with the new key.
3. Change Key A on the HITAG VEGAS read/write device to the new value

Caution: On the data carrier 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 HITAG VEGAS read/write device! (See Chapter 12.5.)

Only after carrying out correctly steps 1 through to 3 (execute a read-access test with the changed key to check it!) may the second key be changed following the steps described above. Conveniently you change both keys to the same value!

5.4.2. Incorrect Procedures Changing Keys

- You change both keys on the read/write device and then try to access the data carrier. That does not work because there is no identity between any of the keys on the data carrier 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 data carrier. This can be possible, only if your system works with both keys and checks one after the other, because one key (here it is Key B) on the data carrier and the read/write device is still identical.

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

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

5.4.3. Changing Logdata

To change logdata use the same procedure as described for changing keys. Be careful to change them by pairs (on the ***HITAG VEGAS*** read/write device and on the data carrier):

1. Change, for example, Logdata 0A on the data carrier (by overwriting page 5).
2. Change Logdata 0A on the read/write device to the new value.
3. Change Logdata 1A on the data carrier (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 HITAG VEGAS read/write device.

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

5.5. Security Mechanism in the VEGAS Read/Write Device

All the data necessary for the authentication of the data carrier and the ***HITAG VEGAS*** read/write device as well as the data needed for encryption can be protected in the ***HITAG VEGAS*** read/write device both from being read and being written using special serial commands.

This mechanism consists of several levels:

Level 0: All security relevant data can be read and written. However, to write these data you have to enter the old data as well. You can read the old data before you start.

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 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, B
Logdata 0A, 0B
Logdata 1A, 1B

You can assign one of the levels mentioned above to each part of information in this list.

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

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00

Appendix: Header File PROLIB5.H (Listing)

Demo-C-Library PROLIB5.H Description

A library programmed in Standard-C with the Borland C++ Compiler Version 3.1. is available on request from B&G.

General Remarks

Communication between the library and the read/write device is provided by the serial interface. This communication is controlled via interrupts. As a consequence a PC-program is not forced into a waiting loop and can execute other functions while the data transfer is running in the background.
To do this, however, some flags are needed:

- RWDEot: Is set to 0 at a library function request and to 1 at the end of the serial protocol.
  This helps to identify the end of the data transmission.

- RWDErr: Saves the error code.
  0 means: errorfree execution
  < 0 means: error processing the commands

- RWDDataLen: Saves the number of data bytes received via the serial interface.
  Can take any value between 0 and 24.

The **PROLIB5.H** file contains short examples to illustrate each of the commands.

Bourgogne et Grasset — ZI Beaune Savigny -– 21200 Beaune – France – Tel. +33 380 26 26 26 – Fax. +33 3 80 26 26 00