LOW LEVEL transfer protocol G200 of TS-HRW series (13.56 MHz)

Version 1.14

GiS
Gesellschaft für Informatik und Steuerungstechnik mbH

Höllochstrasse 1
D-73252 Lenningen
Tel. +49 (0)7026 606 0
Fax +49 (0)7026 606 66
Email rfid@gis-net.de
Homepage http://www.gis-net.de/rfid

Ownership conditions

Changes list:

Doc.	Date	Chapter	Name	Info
1.00	22.05.2007		M. Blank	Start version
1.01	29.11.2007	6, 7, 8, 9	M. Blank	Chapter 6 completed, Chapters 7 – 9 added.
1.06	03.12.2009	7	M. Blank	Additional description and hints added
1.06	22.12.2009	6	M. Blank	Parameter extended
1.07	02.02.2010	6	M. Blank	Parameters for Reader mode extended, several parameter sets for simultaneous reading of Mifare and ISO15693
1.08	03.08.2011	9	M. Blank	Extension for DESFire
1.09	03.07.2013		M. Blank	Extensions for Counters
1.09	10.09.2013	8	M. Blank	Extensions for NFC
1.10	11.02.2013	9	M. Blank	Extension DESFire
1.11	12.11.2014	8	M. Blank	Extension ISO14443B
1.12	18.05.2017		M. Blank	General error correction
1.13	04.12.2018	6	M. Blank	Extensions in Reader mode parameter
1.14	21.08.2019	7	M. Blank	Extensions for ISO15693 parameter

Table of contents

Changes list: *2*

1. Preface *6*

2. Definitions *6*

Interface parameters 6

3. General *7*

General frame 7

Positive Answer 7

Negative Answer 7

4. List of available commands *8*

5. General commands *10*

5.1. GetVersion 10

5.2. Set Baud rate and interface parameters 11

5.3. Set Reader Mode 12

5.4. Set RF 12

5.5. Set IO 13

5.6. Read IO 13

5.7. Read Serial number 14

5.8.Set Config 14

5.9. Get Config 14

5.10. Set Default 15

5.111. Set Communication mode 15

6. Parameter settings for Reader Mode *16*

6.1. Write Mifare® or DESFire® Key 16

6.2. Write parameters 17

6.3. Read Parameter 17

6.4. Write Prefix 19

6.5. Read Prefix 19

6.6. Write Suffix 20

6.7. Read Suffix 20

6.8. Write Termix 20

6.9. Read Termix 21

6.10. Write Postcode 21

6.11. Read Postcode 21

6.12. Write Reader Mode Parameter 22

6.13. Read Reader Mode Parameter 22

Table of contents

7. Commands for ISO15693 Transponder 23

7.1. Set Air protocol 23
7.2. Set Parameter 24
7.3. Get Parameter 25
7.4. ISO Raw Request 26
7.5. ISO 15693 commands 27
7.6. Stay quiet 33
7.7. Read single block 34
7.8. Read single block (Infineon specific) 35
7.9. Write single block 36
7.10. Write single block (Infineon specific) 37
7.11. Lock block 38
7.12. Read multiple blocks 39
7.13. Write multiple blocks 40
7.14. Select 41
7.15. Reset to ready 41
7.16. Write AFI 42
7.17. Lock AFI 42
7.18. Write DSFID 43
7.19. Lock DSFID 43
7.20. Get system info 44
7.21. Get multiple block security status 45
7.22. ISO Write Data (only TS-HMK134 BT old devices) 46
7.23. ISO Check Status (only TS-HMK134 BT old devices) 46

8. Commands for ISO14443-3 (Mifare) Transponder 47

8.1. Request 47
8.2. Select 48
8.3. Halt 49
8.4. Authenticate Mifare Classic 49
8.5. Write Key to E²Prom 51
8.6. Read Block Mifare (Classic and Ultralight) resp. NFC 52
8.7. Write Block Mifare (Classic and Ultralight) resp. NFC 52
8.8. Read value Mifare Classic 53
8.9. Write value (Mifare Classic) 53
8.10. Change Value (Mifare classic) 53
8.11. Sector select Mifare Ultralight resp. NFC Type 2 54
8.12. Request, Wakeup ISO14443B 54
8.13. Attrib ISO14443B 55

Table of contents

9. Commands for ISO14443-4 (DesFire) Transponder.....56

9.1. ISO14443 SetPrologue..... 56
9.2. ISO14443 RATS..... 56
9.3. ISO14443 PPS..... 57
9.4. ISO14443 T=CL Transmit..... 58
9.5. ISO14443 Chaining..... 58

10. Commands to access the HF Reader IC.....59

10.1. Read E²Prom of Controller IC..... 59
10.2. Write E²Prom of Controller IC..... 59
10.3. Read Register of the Controller IC..... 60
10.4. Write Register of the Controller IC..... 60

Common rules

1. Preface

This document describes the commands to communicate with GiS RFID devices of the 13.56 MHz series. The GiS Standard Protocol G200 is used.

Dependent on the device type only parts of the commands are supported.
If a command is used, which is not supported by the device, a NAK error code is delivered.
The device version (see command GetVersion) signals which commands are supported.

22	*ISO Write Data*	*erweitertes Schreiben mehrerer Blöcke (TS-HMK134 BT)*
23	*ISO Check Status*	*Status der ISO Write Data Funktion abfragen (TS-HMK134 BT)*

2. Definitions

Interface parameters

The interface parameters are to be used at all serial connections, also when using USB devices through a Virtual serial port driver.

Baud rate	19200
Parity	no
Data bits	8
Stop bits	1
Protocol	none

Start of Text

	(HEX)
STX	02H

Error codes

OK	00H	No error
DC	14H	Data length not allowed at this command
NAK	15H	No transponder
SYNC	16H	Checksum error
ETB	17H	Collision error
CANCEL	18H	Unknown/Invalid command
EM	19H	CRC Error at air interface

General

3. General

General frame

In communication with the device the general frame is always used in both directions. In the description of the commands the general frame is not shown. Only the data part (CMD, LEN, Data) is shown there.
Command frames with fix and variable length can be used. Only at the answer to the inventory command the command frame with variable length is used in the moment.

Command frame with fixed length

1 Byte	1 Byte	1 Byte	1 Byte	n Bytes			CRC
STX	Address	CMD/ERR	length	Data 1	.....	Data n	Xor
				LSB		MSB	

Command frame with variable length

1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	n Bytes			1 Byte	CRC
STX	Address	CMD/ERR	Block-Mark	length	Data 1	.....	Data n	Block-Mark	Xor
			FF Hex		LSB		MSB	FF Hex	
				this part repeated					

STX	Start of Text
Address	Address of the Slave Module. In case of a RS232 connection **always 01h**.
CMD/ERR	When sending to the device this is the command (CMD). At the answer from the device this is the error code ERR
length	number of data bytes transferred. The 4 header bytes (STX, Address, CMD, length) and the checksum CRC are not counted.
Data 1-n	Data for the command, size as described in length
CRC	XOR with Address, CMD, length and data

Positive Answer

At positive answers the field ERR is always 0.
The meaning of positive answers is described at the corresponding command.

Negative Answer

At negative answers field ERR contains the error code.
The following error codes are possible:

DC4 (14H)	Data length not allowed at this command
NAK (15H)	Command could not be finished correctly. Maybe no transponder was in the field, the transponder has another type or the authentication could not be passed.
SYNC (16H)	Received checksum was wrong.
ETB (17H)	Chip collision occurred
CANCEL (18H)	Command is not existing or not allowed.
EM (19H)	CRC Error at air interface

At the description of the commands the negative answers are not described.

Command list

4. List of available commands

Command (Hex)	Name	Description
General commands		
F0	Device version	Query device version
F2	Set Baud rate	Sets the baud rate
F4	Set Reader Mode	Sets the device to a "pure" reader mode
F5	RF OnOff	Turns antenna field on or off
F6	SetIO	Set outputs, LED's, Buzzer
F7	ReadIO	Read inputs
F8	Read Serial number	Read serial number of the device
F9	Set Config	Set the configuration
FA	Read Config	Read the configuration
FB	Set Default	Set default settings
FF	SetCommunicationMode	Set communication mode (HID⇔ Virtual COM)
Parameter settings for Reader Mode for device version xx2, xx3, xx4, xx5 when device is used as reader only		
80	Write Mifare Key	Save key for data output to device
81	Write Parameter	Set parameters for output of data
82	Write Prefix	Set prefix code to device
83	Write Suffix	set suffix code to device
84	Write Termix	set termix code to device
85	Write Postcode	set postcode to device
86	Write Parameter	set mode parameters for RS232 / USB
89	Read Parameter	read parameters for output of data
8A	Read Prefix	read prefix code from device
8B	Read Suffix	read suffix code from device
8C	Read Termix	read termix code from device
8D	Read Postcode	read postcode from device
8E	Read Parameter	Get mode parameters for RS232 / USB
Pass through commands to RC632 Controller		
05	Read EEPROM	read EEPROM cell of the RC632
06	Write EEPROM	write EEPROM cell of the RC632
07	Read Register	read Register of the RC632
08	Write Register	write Register of the RC632

Command list

Command (Hex)	Name	Description
Commands for ISO15693 Transponder		
20	ISO Raw Request	Common ISO 15693 transfer
21	ISO Air Protocol setting	Set Air Protocol settings
22	ISO Write Data	extended writing of multiple blocks
23	ISO Check Status	Get state of the ISO Write Data function
22	*ISO Write Data*	*Extended writing of several blocks (TS-HMK134 BT)*
23	*ISO Check Status*	*Querying the status of the ISO Write Data (TS-HMK134 BT)*
Commands for ISO1443-3 A Transponder		
30	Mifare Request	Mifare Anticollision Request command
32	Mifare Select	Mifare Select command
32	Mifare Halt	Halt command to stop a Transponders
Commands for Mifare Classic + Ultralight (ISO1443-3 A) Transponder		
33	Mifare Authenticate	Authenticate command for encrypted Transponders
34	Mifare Read	read block
35	Mifare Write	write block
36	Mifare Get Value	read block in value format
37	Mifare Set Value	write block in value format
38	Mifare Change Value	change value
39	Mifare Write Key	write key (save in EEPROM)
3A	Mifare Sector Select	Select a Sector for block numbers above 255
Commands for ISO1443-4 A (T=CL) Transponder		
40	Mifare Set Prologue	set prologue data for ISO14443-4 protocol
41	ISO14443 RATS	RATS command, switch to ISO14443-4 mode
42	ISO14443 PPS	Set data transfer speed
45	Transceiver	Common ISO14443-4 access T=CL raw request
46	Chaining	Reading of additional data, if Transceiver has announced more data

General commands

5. General commands

5.1. GetVersion

Reading of device version

CMD	Length	Data
F0h	0	no Data

Positive answer:

ERR	Length	Data 1 – 3	Data 4
0	4	Device number 001 – 999 (ASCII)	Firmware Version (ASCII)

By reading the device number the supported commands can be selected.

Type	Device number	supported commands
TS-HW3x	121	Commands for ISO 15693
TS-HRW3x	123 125	Commands for ISO 15693 also Commands for Reader Mode
TS-HR3x	122 124	Commands for Reader Mode
TS-HRW90	135	Commands for ISO 15693 also Commands for Reader Mode
TS-HW36	141	Commands for ISO 15693
TS-HR36	144	Commands for Reader Mode
TS-HRW36	145	Commands for ISO 15693 also Commands for Reader Mode
TS-HML134 BT	155	Commands for ISO 15693 also Commands for Reader Mode
TS-HW38	161	Commands for ISO 15693 and Mifare
TS-HR38	164	Commands for Reader Mode with Mifare
TS-HRW38	165	Commands for ISO 15693 and Mifare also Commands for Reader Mode
TS-HRW32	195	Commands for ISO 15693 and Mifare also Commands for Reader Mode
TS-HRW390 TS-HRW395	405	Commands for ISO 15693 and Mifare also Commands for Reader Mode

The Firmware version is coded as follows:
'0' – '9', 'A' – 'Z', 'a' – 'z' is equal to 0-9, 10-35, 36-61

General commands

5.2. Set Baud rate and interface parameters

With this command the communication parameters are changed permanently.

CMD	Length	Data
F2h	1	Baud rate

Both the baud rate and the parity mode are coded in baud rate.
The lower 4 bits contain the baud rate, the upper 4 bits contain the parity mode.

Baud rate	
00H	2400 Baud
01H	4800 Baud
02H	9600 Baud
03H	19200 Baud
04H	38400 Baud
05H	57600 Baud
06H	115200 Baud
07H	230400 Baud
08H	460800 Baud
09H	921600 Baud

Parity mode		
	Stop Bits	Parity
00H	1	no
10H	1	even
20H	1	odd
30H	2	no

Default value at delivery is 03 (19200 Baud, No Parity, 1 Stop bit, 8 Data bits).
Attention: The answer to this command is sent with the old settings.
Immediately after the answer is send, the device changes to the new settings.
This command is allowed only at RS232 devices, not at USB devices.
Not all devices support all baud rates!

Positive answer:

ERR	Length	Data
0	0	no Data

General commands

5.3. Set Reader Mode

Set the device to reader or programmer mode.
In reader mot the device sends the transponder data automatically depending on the settings without protocol frame.

CMD	Length	Data
F4h	1	Reader Mode 0: Programmer Mode 1: Reader Mode 2: switch to Power Up Mode 80H: set Programmer Mode as Power UP Mode 81H: set Reader Mode as Power UP Mode

The settings 2, 80H und 81H are not supported at all devices

Positive answer:

ERR	Length	Data
0	0	no Data

5.3.1. Read Power UP Mode (only for devices with HID Interface)

With this command, the Power UP Mode is read

CMD	Length	Data
F4h	0	no Data

Positive answer:

ERR	Length	Data
0	1	Power UP Mode 80H: Programmer Mode set as Power UP Mode 81H: Reader Mode set as Power UP Mode

5.4. Set RF

With this command the antenna field is turned on or off.
Please respect, that some commands set the antenna field automatically. This command can be used to turn the antenna field off to save energy or to reset the transponder in the field. (Turn field off and on).

CMD	Length	Data
F5h	1	RF Mode 0: turn antenna field off 1: turn antenna field on

Positive answer:

ERR	Length	Data
0	0	no Data

General commands

5.5. Set IO

Set the outputs of the device. Depending on the device different outputs are available. After power on the LED's are set automatically. After using this command only those outputs are set automatically which are not included in the mask.

CMD	Length	Data 1	Data 2
F6h	2	Mask	Data

In Mask you have to set all bits which are to be changed through the command. in data all output which have to be set are set to 1 and all outputs which have to be cleared are set to 0.
Definition of bits:

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
LED yellow	LED green	LED red	Buzzer	Out 3	Out 2	Out 1	Out 0

Positive answer:

ERR	Length	Data
0	0	no Data

If the device is equipped with a relay output, this is connected through Out 0.

Example: Mask: C0H Data: 40H
set the green LED and clear the yellow LED, the red LED and all other outputs keep unchanged and are set through the reader depending on the operation mode.

5.6. Read IO

Reads the inputs of the device. Depending on the device, different inputs can be available.

CMD	Length	Data
F7h	0	no Data

Positive answer:

ERR	Length	Data 1
0	1	Data

The data bits are used as follows:

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
In 7	In 6	In 5	In 4	In 3	In 2	In 1	In 0

If the device is equipped with a sensor input, this is available in In 0.

General commands

5.7. Read Serial number

This command reads the serial number from the device

CMD	Length	Data
F8h	0	no Data

Positive answer:

ERR	Length	Data 1 – 4
0	4	Serial number (binary)

5.8.Set Config

Write the configuration to the device. The configuration values are different at the devices. This function is not supported at all devices.

CMD	Length	Data 1 – n
F9h	n	Configuration

Positive answer:

ERR	Length	Data
0	0	no Data

5.9. Get Config

Read the configuration from the device. The configuration values are different at the devices. This function is not supported at all devices.

CMD	Length	Data
FAh	0	no Data

Positive answer:

ERR	Length	Data 1 – n
0	n	Configuration

General commands

5.10. Set Default

Set the Firmware default setting in the device. This function is not supported at all devices.

CMD	Length	Data
FBh	0	no Data

Positive answer:

ERR	Length	Data
0	0	no Data

5.111. Set Communication mode

Set the communication mode (only at USB HID/VCOM devices)

CMD	Length	Data 1
FFh	1	Mode

Mode New communication mode
1: HID
2: Virtual COM

Positive answer:

ERR	Length	Data
0	0	no Data

Reader Mode

6. Parameter settings for Reader Mode

These commands are used to set the parameters for the device to be used in reader mode.

6.1. Write Mifare® or DESFire® Key

With this command the key to access the Mifare® or DESFire® Transponder is stored in the device.
This key works only during access to registers of Mifare® transponders with Crypto engine (Mifare 1K, Mifare 4K)
or access to DESFire® transponders during access to encrypted files or CardUID

CMD	Length	Data 1	Data 2 – 7 (17)
80h	7 or 17	KeyType	Key

Key Type — Bits 0 – 3 Key type
0 = Mifare Classic KeyA,
1 = Mifare Classic KeyB,
2 = DESFire 3DES Key,
3 = DESFire AES Key
Bits 4 – 8 Key number, only used at DESFire

Key — 6 or 16 Byte Key information, LSB first
Key is 6 Byte if Mifare Key (KeyA orKeyB) and 16 Byte if DESFire 3DES or AES Key.

Positive answer:

ERR	Length	Data
0	0	no Data

Reader Mode

6.2. Write parameters

CMD	Length	Data 1- n
81h	n	Data Structure

Positive answer:

ERR	Length	Data
0	0	no Data

6.3. Read Parameter

CMD	Length	Data
89h	0	no Data

Positive answer:

ERR	Length	Data 1- n
0	n	Data Structure

Most TS-HRW devices support only one parameter data structure. The size of this structure might be different depending on the device.
Only TS-HRW38 with Firmware Version 9 and TS-HRW32 may have multiple parameter data structures. Using this the given transponder types are alternated.
Depending on the device maybe only the first bytes of the data structure are given. If multiple data structures are given, all structures have to be set with 20 Byte per data structure.

Reader Mode

6.3.1 Data Structure:

The parameter for reading and writing are passed always in the same order.

Pos.	length	Name	*Description*
0	1	Wait	*Wait time* between 2 characters: (0 – 127) Only PS/2. Wait time = **N/2** in milliseconds. Default = 10
1	1	TTyp	*Transpondertyp:* Bit 0 – 5 0 = UID ISO15693 1 = Register ISO15693 2 = UID Mifare 3 = Register Mifare 4 = UID ICode1 5 = Register ICode1 6 = UID DESFire 7 = File content DESFire Bit 6: 0 = normal 1 = bitweise gespiegelt Bit 7 0 = LSB first 1 = MSB first (Byteweise gedreht)
2	5	Register	The entry consists always of 4 Register data bytes and the end identification 0xffH (5th Byte). This entry is only valid if a "Register" type is selected in TTyp (1 or 3). Byte 5 is always the end identification 0xffH. z.B. 0x00,0x01,0x0f,0x05,0xff. If TTyp 7 File content DESFire is used, the first 3 byte define the Application ID and the 4th Byte defines the FileID.
7	1	DTyp	*Data type:* 0 = Hexadecimal, 3 = Decimal without leading zero, 1 = decimal, 4 = Hexadecimal with lower case letters 2 = ASCII, 5 = ASCII, 00H will be suppressed, do not fill with SPACE
8	1	Zeichen	*Number of characters. (1–32).* Defines how much characters are transferred per block.
9	1	Frequenz	*Frequency.* Only for PS/2. Here we transfer a special interval time span. You can calculate the frequency with the formula: $f[MHz] = \frac{1}{(64[\mu s] + 8[\mu s] * N)}$. The value 5 is correlating with frequency 10 kHz. (Default) The value 17 is correlating with frequency 5 kHz. (Values are rounded).
10	1	Timeout	You can calculate the time out with the following formula: (Only for PS/2): T[ms] = 30[ms] + 30[ms] * Timeout. Default value is 5, which means 180 ms. After this time is gone, the same transponder can be read again.
11	1	ValidBytes	(1-16) Number of bytes used in UID or data blocks. With this, the upper bits of the UID can be masked out. Default value is 5
12	1	ValidFrom	(1-16) Start byte from which the data is transferred. This is only available at TS-HR38 with Version 1.07 or higher or TS-HR32.
13	1	TypKenn1	Detection characters for the transponder type are transmitted before the data, 1 ASCII character, at 0 nothing is transferred.
14	1	TypKenn2	Detection characters for the transponder type is transmitted according to the data, 1 ASCII character, at 0 nothing is transferred.
15	1	DesfireMode	0:plain, 1:Authenticated, 2:with MAC, 3:fully encrypted
16	4	-	Reserve, default value 0

Reader Mode

6.4. Write Prefix

The prefix is transferred before the Transponder data is sent.

CMD	Length	Data 1 – n
82h	n	Prefix

Prefix: maximum 31 characters plus end marker 0xffH.

Positive answer:

ERR	Length	Data
0	0	no Data

6.5. Read Prefix

The prefix is transferred before the Transponder Data is sent.

CMD	Length	Data
8Ah	0	no Data

Positive answer:

ERR	Length	Data 1 – n
0	n	Prefix

Prefix: maximum 31 characters plus end marker 0xffH.

Reader Mode

6.6. Write Suffix

The suffix is transferred after the Transponder data is sent.

CMD	Length	Data 1 – n
83h	n	Suffix

Suffix: maximum 31 characters plus end marker 0xffH.

Positive answer:

ERR	Length	Data
0	0	no Data

6.7. Read Suffix

The suffix is transferred after the Transponder data is sent.

CMD	Length	Data
8Bh	0	no Data

Positive answer:

ERR	Length	Data 1 – n
0	n	Suffix

Suffix: maximum 31 characters plus end marker 0xffH.

6.8. Write Termix

The termix is transferred between the Transponder register data blocks.

CMD	Length	Data 1 – n
84h	n	Termix

Termix: maximum 31 characters plus end marker 0xffH.

Positive answer:

ERR	Length	Data
0	0	no Data

Reader Mode

6.9. Read Termix

The termix is transferred between the Transponder register data blocks.

CMD	Length	Data
8Ch	0	no Data

Positive answer:

ERR	Length	Data 1 – n
0	n	Termix

Termix: maximum 31 characters plus end marker 0xffH.

6.10. Write Postcode

The postcode is transferred when the transponder is removed

CMD	Length	Data 1 – n
85h	n	Postcode

Postcode: maximum 31 characters plus end marker 0xffH.

Positive answer:

ERR	Length	Data
0	0	no Data

6.11. Read Postcode

The postcode is transferred when the transponder is removed

CMD	Length	Data
8Dh	0	no Data

Positive answer:

ERR	Length	Data 1 – n
0	n	Postcode

Postcode: maximum 31 characters plus end marker 0xffH.

Reader Mode

6.12. Write Reader Mode Parameter

CMD	Length	Data 1	Data 2	Data 3	Data 4
86h	4	Mode	Cycle Time	Requirement	Timeout

Mode: operation mode
0: Send data when transponder is entering or leaving field.
1: Send data on request.
The request character is defined in **Requirement**.
The device sense data when the request character is transmitted to the device.
3: Send data cyclic

Cycle Time: The time is given in tenth of seconds. The default value is 10, this means 1 Second. Then cycle time is only valid in mode 3.

Requirement: Request character which is active only in mode 1. Default value '**?**' (3fH)

Timeout: The time is given in tenth of seconds. The default value is 20, this means 2 seconds. Then timeout is valid only in mode 0. It defines how long a transponder has to be out of field to be recognized again as new transponder.

Positive answer:

ERR	Length	Data
0	0	no Data

6.13. Read Reader Mode Parameter

CMD	Length	Data
8Eh	0	no Data

Positive answer:

ERR	Length	Data 1	Data 2	Data 3	Data 4
0	4	Mode	Cycle Time	Requirement	Timeout

The meaning of the parameters is as described in write Reader mode parameter

Commands for ISO15693 Transponder

7. Commands for ISO15693 Transponder

These commands are only supported at devices which have writing functions enabled.
This can be derived from the device version.

7.1. Set Air protocol

CMD	Length	Data 1
21h	1	Data

The data bits are used as follows:

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
-	-	-	-	-	Data coding mode	-	Request Modulation

"Request Modulation" sets the Modulation type for ISO15693 requests.
0 means 10% ASK
1 means 100% ASK

"Data coding mode" sets the ISO15693 "Data coding" type.
0 means 1:4
1 means 1:256,

The default value should be 0x01.
Request Modulation= 100% ASK and Data coding mode = 1:4.

Positive answer:

ERR	Length	Data
0	0	no Data

7.2. Set Parameter

Write the configuration parameters to the device. Possible configuration values vary depending on the device. This function is not supported by all devices.

CMD	Length	Data 1 – n
22h	n	Parameter

Positive answer:

ERR	Length	Data
0	0	no Data

7.2.1. Parameter for TS-HRW390

With TS-HRW390 (from V1.02) various settings of the RF Controller can be set.
Structure of the parameter data:

Designation	Length	Description
Mode	1 Byte	Bitwise coding of the parameter data used. If the respective bit is set, the corresponding setting follows, otherwise this setting is not contained in the data, i.e. the data is correspondingly shorter. Bit 0: Minimum Level follows Bit 1: Collision Level follows Bit 2: Amplification follows
Minimum Level	1 Byte	Minimum signal strength at decoder input for valid signal. 0 – 7: Setting the value 0xFF: Setting to default company setting
Collision Level	1 Byte	Minimum signal strength for weaker bit for collision detection. 0 – 7: Setting the value 0xFF: Setting to default company setting
Amplification	1 Byte	Verstärkung der letzten Verstärkerstufe 0 – 7: Setting the value 0xFF: Setting to default company setting

Commands for ISO15693 Transponder

7.3. Get Parameter

Read the configuration parameters from the device. Possible configuration values vary depending on the device. This function is not supported by all devices.

CMD	Length	Data
23h	0 or 1	Mode

Positive answer:

ERR	Length	Data 1 – n
0	n	Parameter

If the optional parameter Mode is specified with Get Parameter, only the data according to the set bits are included in the response data.

7.3.1. Parameter for TS-HRW390

With TS-HRW390 (from V1.02) various settings of the RF Controller can be read.
Structure of the parameter data:

Designation	Length	Description
Mode	1 Byte	Bitwise coding of the parameter data used. If the respective bit is set, the corresponding setting follows, otherwise this setting is not contained in the data, i.e. the data is correspondingly shorter. Bit 0: Minimum Level follows Bit 1: Collision Level follows Bit 2: Amplification follows
Minimum Level	1 Byte	Minimum signal strength at decoder input for valid signal. 0 – 7: Setting the value
Collision Level	1 Byte	Minimum signal strength for weaker bit for collision detection. 0 – 7: Setting the value
Amplification	1 Byte	Amplification of the last amplifier stage 0 – 7: Setting the value

Commands for ISO15693 Transponder

7.4. ISO Raw Request

This is the general command frame for all ISO 15693 commands.
With this all commands for ISO15693 Transponder can be sent transparently.
For a detailed description of the commands the document:
“ISO/IEC 15693-3 (First Edition 2001-04-01) Part 3: Anti-collision and transmission protocol”
has to be used.

CMD	Length	Data 1 - n
20h	n	depending on command

Data: the transferred data depends on the command which is transferred to the transponder

Positive answer:

ERR	Length	Data 1 – n
0	n	depending on answer

Data: The transferred data depends on the answer which is received form the transponder.

Attention:
Not all ISO15693 transponders support all commands. Regarding to the ISO 15693 specification a transponder type has to support only the inventory and stay quiet command. All other commands are optional. For a detailed description of supported commands please use the documentation of the used transponder type.

Commands for ISO15693 Transponder

7.5. ISO 15693 commands

Here only the data part of the commands is shown, without the general command frame.

Inventory

Data	Length	Meaning
1	**1 Byte**	0xXX ISO Request Flags
2	**1 Byte**	0x01 Inventory ISO Command
3	**1 Byte**	AFI Value, optional
4 (3)	**1 Byte**	0x00 ISO Data

The AFI Value is allowed to be transmitted only, if the AFI Flag is set in the Request Flags.

Description of the ISO Request Flag Bit's

	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Data 1	RFU	Option	Length Slots	AFI	Protocol	Inventory	Data Rate	Sub Carrier

Attention:
If the inventory command is used, Bit2 (Inventory) in ISO Request Flag has to be set to 1, otherwise the command returns an error.

Sub-Carrier = 0
Sub-Carrier = 1 (recommended)
Data Rate = 0 (Low Data Rate) (recommended)
Data Rate = 1 (High Data Rate)
Inventory = 1
Length Slots = 0 (16 Slots)
Length Slots = 1 (1 Slot)
All other Bits have to be set to 0 (Null)

Normally the ISO Request Flag is set to 0x25 to read a single slot and set to 0x05 to do a 16 slot inventory.

Commands for ISO15693 Transponder

Common inventory answer

The answer to the inventory command is a special case, because a variable length answer is used depending of the found transponders in the field.
Hereby several sub blocks are contained in the answer.
The data is separated for each of the 16 "Timeslots".
The Frame is as described in "Command frame with variable length" in the General section.

In the data of each "Timeslots" at least the Slot-Parameter is contained. All other fields are optional.

Data	**Length**	Meaning
1	1 Byte	Slot-Parameter
2	1 Byte	Response Flag
3	1 Byte	DSFID / ISO Error flag
4 – 11	8 Byte	UID Data

Description of Slot-Parameter

	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Data 0	Slot Number				Error code 0 = no error 1 = no transponder 2 = Collision 8 = Checksum error			

Commands for ISO15693 Transponder

Description of the response flag

	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Data 1	RFU	RFU	RFU	RFU	RFU	RFU	RFU	Error flag

Error flag = 0 no error
Error flag = 1 error, Data 2 is ISO Error flag (Response Error)

Error Code	ISO Description	Description
0x01	Command not supported	Command is not supported by tag
0x02	Command not recognized	Command not recognized by tag
0x03	Wrong option	Option flag not allowed at this command
0x0F	No information	general error
0x10	Block not available	Block is not available (not existing)
0x11	Block already locked	Block is already locked and can not be locked anymore
0x12	Block is locked (no change possible)	Block is locked and cannot be changed
0x13	Block not successfully programmed	Block could not be programmed
0x14	Block was not successfully locked	Block could not be locked
0xA0 to 0xDF	Custom command error code	Custom error depends on chip manufacturer
all others	RFU	Reserved for future use

See also **ISO/IEC 15693-3** Specification (Table 7)

Commands for ISO15693 Transponder

Example 1:
Single slot Inventory command
Send: 02 01 20 03 25 01 00 bcc
Receive: 02 01 00 ff 0b 00 00 00 5d 50 7a 01 00 00 07 e0 ff bcc

Transponder with UID (5d 50 7a 01 00 00 07 e0) is in 1st slot.

Example 2:
16 Slot Inventory command
Send: 02 01 20 03 05 01 00 bcc
Receive: 02 01 00 ff 01 01 01 11 01 21 01 31 01 41 01 51 01 61 01 71 01 81 01 91 01 a1 01 b1 01 c1 0b d0 00 00 5d 50 7a 01 00 00 07 e0 01 e1 01 f1 ff bcc

The slots 0 - 12 and 14 - 15 return the Length of 1 and the Slot Parameter Byte gives Error code 1(no Transponder found) und die Slot Number.

In the answer of Slot 13 the following data is found:

Length	= 0x0b (11 Byte follow)
Slot Parameter	= 0xd0 (no error and Slot number 13)
Response-Flags	= 0x00 (no error)
DSFID	= 0x00
Data 4 to Data 11	= 5d 50 7a 01 00 00 07 e0 (UID)

Transponder with UID (5d 50 7a 01 00 00 07 e0) is found in Slot 13.

If no transponder would be found in any Slot, the following data would have been received at the 16 Slot Inventory command.

Receive: 02 01 ff 20 01 01 01 11 01 21 01 31 01 41 01 51 01 61 01 71 01 81 01 91 01 a1 01 b1 01 c1 01 d1 01 e1 01 f1 ff bcc
All 16 Slots return error 1 (no transponder found)

Commands for ISO15693 Transponder

Attention:

At this place again the **ISO Request Flag** (send) and **Response Flag** (receive) are described. IN all following commands this description if valid if the flags are used!

Description of the ISO Request Flag

	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Data 1	RFU	Option	Address	Select	Protocol	Inventory	Data Rate	Sub Carrier

Attention:

In none of the following commands Bit2 (Inventory) should be set, otherwise the command is not interpreted correctly and will return an error.
If a command is used with UID, it is absolutely necessary, that Bit5 (Address) is set, otherwise the command returns with an error.

Sub-Carrier = 0 (Single sub carrier)
Sub-Carrier = 1 (Two sub carriers) (recommended)
Data Rate = 0 (Low Data Rate) (recommended)
Data Rate = 1 (High Data Rate)
Inventory = 0 (necessary)
Address = 0 (Transponder – Addressing without UID)
Address = 1 (Transponder – Addressing with UID)
Option = 0 (if no other value is given at the command)
Option = 1 (meaning of the flag described at the command)
All other bits are to be set to 0 (Null)

Commands for ISO15693 Transponder

Meaning of Response Flag

	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Data 1	RFU	RFU	RFU	RFU	RFU	RFU	RFU	Error flag

Error flag = 0 no error
Error flag = 1 error, the next byte (Data 2) is ISO Error flag (Response Error)

Error Code	ISO Description	Description
0x01	Command not supported	Command is not supported by tag
0x02	Command not recognized	Command not recognized by tag
0x03	Wrong option	Option flag not allowed at this command
0x0F	No information	general error
0x10	Block not available	Block is not available (not existing)
0x11	Block already locked	Block is already locked and can not be locked anymore
0x12	Block is locked (no change possible)	Block is locked and cannot be changed
0x13	Block not successfully programmed	Block could not be programmed
0x14	Block was not successfully locked	Block could not be locked
0xA0 to 0xDF	Custom command error code	Custom error depends on chip manufacturer
all others	RFU	Reserved for future use

See also **ISO/IEC 15693-3** Specification (Table 7)

Attention:
This is an answer to an ISO command if an error in the chip protocol occurred.
This is valid for all of the following ISO commands

Answer	
Reader error	0x00
Response Flag	0x01
Response Error	0xXX ISO error

Commands for ISO15693 Transponder

7.6. Stay quiet

Data	Length	Meaning
1	**1**	ISO Request Flag
2	**1**	0x02 Stay quiet ISO Command
3 – 10	**8**	xxxx UID

Example:
Send: 02 01 20 0a 21 02 5d 50 7a 01 00 00 07 e0 bcc
Receive: 02 01 00 01 01 bcc

Note:
The “Stay Quiet” command is used stop the transponder from answering to the “Inventory” command. To use “Stay Quiet” the UID of the transponder has to be given. This state is turned off with the command: “ResetToReady“ or by talking to the transponder with and command with UID. For example ReadSingleBlock with UID.

“Stay quiet” gives always the answer “No transponder found”

Commands for ISO15693 Transponder

7.7. Read single block

Data	Length	Meaning
1	**1**	ISO Request Flag
2	**1**	0x20 Read Single Block ISO Command
3 – 10	**8**	xxxx UID optional
3 or 11	**1**	xx Block number

Answer:

Data	Length	Meaning
1	**1**	Reader error
2	**1**	Response Flag
3	**1**	**Block Security Status (optional**, if Option Flag in Request Flags is set**)**
4(3) – n	**x**	Block content

Description of Block Security State

	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Byte	RFU	RFU	RFU	RFU	RFU	RFU	RFU	Lockflag

Lockflag = 0 the Transponder block is not write protected (not locked)
Lockflag = 1 the Transponder block is write protected (locked)

Example 1:
Reading of Block 0 with UID and without Option Flag
Send: 02 01 20 0b 21 20 5d 50 7a 01 00 00 07 e0 00 bcc
Receive: 02 01 00 06 00 00 12 34 56 78 bcc

The contents of Block 0 are 4 Bytes with the values 0x12, 0x34, 0x56 and 0x78.

Commands for ISO15693 Transponder

7.8. Read single block (Infineon specific)

Data	Length	Meaning
1	**1**	ISO Request Flag
2	**1**	0xA0 Custom ISO Command
3	**1**	0x05 IC manufacturer Code
4-11	**8**	UID optional
12 (4)	**1**	0x10 Read single block command
13 (5)	**1**	xx Block number
14 (6)	**1**	0x00

Answer:

Data	Length	Meaning
1	**1**	Reader Fehler
2	**1**	Response Flag
3 – n	**x**	Block contents

Example 1:
Reading of Block 4 with UID and without Option Flag
Send: 02 01 20 0e 23 a0 05 38 0A AD 00 00 05 05 60 10 **04** 00 bcc
Receive: 02 01 00 0a 00 00 aa aa aa aa aa aa aa aa bcc

The contents of Block 4 are 8 Bytes with the values 0xaa, 0xaa, 0xaa, 0xaa, 0xaa, 0xaa, 0xaa, 0xaa.

Commands for ISO15693 Transponder

7.9. Write single block

Data	Length	Meaning
1	**1**	ISO Request Flag
2	**1**	0x21 Write Single Block ISO Command
3 – 10	**8**	xxxx UID optional
3 or 11	**1**	xx Block number
4 (12)	**n**	Transponder Data

Answer:

Data	Length	Meaning
1	**1**	Reader error
2	**1**	Response Flag
3	**1**	Response Error optional

Example 1:
Writing of Data in Block 1 with UID
Send:02 01 20 0f 61 21 5d 50 70 01 00 00 07 e0 **01** 12 34 56 78 bcc
Receive: 02 01 00 02 00 00 bcc

Block 1 has been written with 4 Bytes with values 0x12, 0x34, 0x56 und 0x78.

Note:
This Example was made with a Texas Instruments Transponder. Because of this the Option Flag in ISO Request Flags has to be set. At this transponder type this is necessary.

Some transponder types do not send the answer to a write command within the given time and so a negative answer (NAK = no transponder) is created.
To make sure, the write command was successful, a "read after write" has to be done by issuing a read command to the requested block and comparing the result.

Commands for ISO15693 Transponder

7.10. Write single block (Infineon specific)

Data	Length	Meaning
1	**1**	ISO Request Flag
2	**1**	0xA0 Custom ISO Command
3	**1**	0x05 IC Manufacturer code
4	**8**	UID optional
12 (4)	**1**	0x30 Write single block command
13 (5)	**1**	Block number
14 (6)	**1**	0x00
15 (7)	**n**	Transponder Data

Answer:

Data	Length	Meaning
1	**1**	Reader error
2	**1**	Response Flag
3	**1**	Response Error optional

Example 1:
Write Data to Block 4 with UID
Send: 02 01 20 16 0b a0 05 38 0A AD 00 00 05 05 60 30 **04** 00 12 12 12 12 12 12 12 12 bcc
Receive: 02 01 00 02 00 00 bcc

Block 4 has been written with 8 Bytes with values 0x12, 0x12, 0x12, 0x12, 0x12, 0x12, 0x12, 0x12.

Note:
At the Infineon Transponder “My – D” the blocks 0,1,2 are declared as „Service Area“.
These blocks cannot be written.

Commands for ISO15693 Transponder

7.11. Lock block

Data	Length	Meaning
1	**1**	ISO Request Flag
2	**1**	0x21 Lock Block ISO Command
3 – 10	**8**	xxxx UID
11	**1**	xx Block number

Answer:

Data	Length	Meaning
1	**1**	Reader error
2	**1**	Response Flag
3	**1**	Response Error optional

Example 1:
Lock Block 5 with UID
Send: 02 01 20 0b 00 61 22 5d 50 7a 01 00 00 07 e0 **05** bcc (Texas Instruments Transponder)
Send: 02 01 20 0b 00 21 22 5d 50 7a 01 00 00 07 e0 **05** bcc
Receive: 02 01 00 02 00 00 bcc

Block 5 is write protected.
Attention: This process is irreversible.

Note:
Using the command “Read Single Block” the “Block Security State” can be read using the option flag. So you can see if the block is write protected or not. Also you can use “Get multiple security state”.
At a Texas Instruments Transponder the Option Flag in ISO Request Flags has to be set. At this transponder type this is necessary.

Description of the Block Security State

	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Byte	RFU	RFU	RFU	RFU	RFU	RFU	RFU	Lockflag

Lockflag = 0 the Transponder is not write protected (Not Locked)
Lockflag = 1 the Transponder is write protected (Locked)

Commands for ISO15693 Transponder

7.12. Read multiple blocks

Data	Length	Meaning
1	**1**	ISO Request Flag
2	**1**	0x23 Read multiple blocks ISO Command
3 – 10	**8**	xxxx UID optional
3 or 11	**1**	xx Start block number
4 or 12	**1**	xx Block Length

Answer:

Data	Length	Meaning
1	**1**	Reader error
2	**1**	Response Flag
3 – x	**n**	Response error if Response Flag is set otherwise Block content

Example 1:
Reading of Block 0 to Block 2 with UID und without Option Flag
Send: 02 01 20 0c 21 23 5d 50 70 01 00 00 07 e0 **00 02** bcc
Receive: 02 01 00 0e 00 00 55 55 55 55 30 30 30 31 30 30 30 30 bcc

Note:
Block length is one below the actually read blocks.
This is predefined in the **ISO/IEC 15693-3** Specification.
This means, using block length 0 reads one block, block length 2 reads 3 blocks.

Commands for ISO15693 Transponder

7.13. Write multiple blocks

Data	Length	Meaning
1	**1**	ISO Request Flag
2	**1**	0x24 Write Multiple Block ISO Command
3 – 10	**8**	xxxx UID optional
3 or 11	**1**	xx Start block number
4 or 12	**1**	xx Block Length
5 (13)	**n**	Transponder Data

Answer:

Data	Length	Meaning
1	**1**	Reader error
2	**1**	Response Flag
3	**1**	Response Error optional

Example 1:
Writing of Block 0 to Block 1 with UID and without Option Flag
Send: 02 01 20 14 21 24 5d 50 70 01 00 00 07 e0 **00 01** 12 34 56 78 44 44 44 44 bcc
Receive: 02 01 00 02 00 00 bcc

Note:
Block length is one below the actually read blocks.
This is predefined in the **ISO/IEC 15693-3** Specification.
This means, using block length 0 writes one block, block length 1 writes 2 blocks.

Some transponder types do not send the answer to a write command within the given time and so a negative answer (NAK = no transponder) is created.
To make sure, the write command was successful, a "read after write" has to be done by issuing a read command to the requested blocks and comparing the result.

Commands for ISO15693 Transponder

7.14. Select

Data	Length	Meaning
1	1	ISO Request Flag
2	1	0x25 Select ISO Command
3 – 10	8	xxxx UID

Answer:

Data	Length	Meaning
1	1	Reader error
2	1	Response Flag
3	1	Response Error optional

Example 1:
Select a Transponder with UID
Send: 02 01 20 0a 21 25 5d 50 70 01 00 00 07 e0 bcc
Receive: 02 01 00 02 00 00 bcc

Example 2:
Select a Transponder with UID
Send: 02 01 20 0a 21 25 5d 50 70 01 00 00 07 e0 bcc
Receive: 02 01 00 01 01 bcc (Reader error) Transponder has not the same UID

Example 3:
Select a Transponder with UID
Send: 02 01 20 0a 21 25 5d 50 70 01 00 00 07 e0 bcc
Receive: 02 01 00 02 00 xx bcc (Response Flag error)

7.15. Reset to ready

Data	Length	Meaning
1	1	ISO Request Flag
2	1	0x26 Reset to ready ISO Command
3 – 10	8	xxxx UID

Answer:

Data	Length	Meaning
1	1	Reader error
2	1	Response Flag
3	1	Response Error optional

Example 1:
Reset to ready with UID discards the Stay quiet State
Send: 02 01 20 0a 21 26 5d 50 70 01 00 00 07 e0 bcc
Receive: 02 01 00 02 00 00 bcc

Commands for ISO15693 Transponder

7.16. Write AFI

Data	Length	Meaning
1	**1**	ISO Request Flag
2	**1**	0x27 Write AFI ISO Command
3 – 10	**8**	xxxx UID optional
3 or 11	**1**	AFI

Answer:

Data	Length	Meaning
1	**1**	Reader error
2	**1**	Response Flag
3	**1**	Response Error optional

Example 1:
Write AFI Coding of a Transport Transponders with UID
Send: 02 01 20 0b 21 27 5d 50 70 01 00 00 07 e0 **10** bcc
Receive: 02 01 00 02 00 00 bcc

Note:
The complete coding of the AFI Flags is described in the **ISO/IEC 15693-3** Specification.

7.17. Lock AFI

Data	Length	Meaning
1	**1**	ISO Request Flag
2	**1**	0x28 Lock AFI ISO Command
3 – 10	**8**	xxxx UID optional

Answer:

Data	Length	Meaning
1	**1**	Reader error
2	**1**	Response Flag
3	**1**	Response Error optional

Example 1:
Write protection for the AFI Flag with UID
Send: 02 01 20 0a 21 28 5d 50 70 01 00 00 07 e0 bcc
Receive: 02 01 00 02 00 00 bcc

Commands for ISO15693 Transponder

7.18. Write DSFID

Data	Length	Meaning
1	**1**	ISO Request Flag
2	**1**	0x29 Write DSFID ISO Command
3 – 10	**8**	xxxx UID optional
3 or 11	**1**	DSFID Flag

Answer:

Data	Length	Meaning
1	**1**	Leser Fehler
2	**1**	Response Flag
3	**1**	Response Error optional

Example 1:
Write freely defined DSFID Coding of a Transponders with UID
Send: 02 01 20 0b 21 29 5d 50 70 01 00 00 07 e0 **20** bcc
Receive: 02 01 00 02 00 00 bcc

Note:
The complete coding of DSFID Flags if free defined, the meaning of the bits has to be user define (see **ISO/IEC 15693-3** Specification).

7.19. Lock DSFID

Data	Length	Meaning
1	**1**	ISO Request Flag
2	**1**	0x2a Lock DSFID ISO Command
3 – 10	**8**	xxxx UID optional

Answer:

Data	Length	Meaning
1	**1**	Reader error
2	**1**	Response Flag
3	**1**	Response Error optional

Example 1:
Write write protection for the DSFID Flag with UID
Send: 02 01 20 0a 21 2a 5d 50 70 01 00 00 07 e0 bcc
Receive: 02 01 00 02 00 00 bcc

Commands for ISO15693 Transponder

7.20. Get system info

Data	Length	Meaning
1	**1**	ISO Request Flag
2	**1**	0x2b GetSystemInfo ISO Command
3 – 10	**8**	xxxx UID optional

Answer:

Data	Length	Meaning
1	**1**	Reader error
2	**1**	Response Flag
3	**1**	Info Flag / Response Error
4 – 11	**8**	UID
	1	DSFID optional if DSFID Bit set
	1	AFI optional if AFI Bit set
	1	Block Length optional if memory size Bit set
	1	Bytes per Block optional if memory size Bit set
	1	IC Reference optional if IC-Ref. Bit set.

Description of Info Flags

	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Byte 3	RFU	RFU	RFU	RFU	IC Ref.	memory size	AFI	DSFID

Description of Bytes, if memory size Bit set in Info Flag

	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Byte x	Block Length							
	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Byte x+1	RFU	RFU	RFU	Bytes per Block				

Example 1:
Read System Info of a Transponder with UID
Send: 02 01 20 0a 21 2b 5d 50 70 01 00 00 07 e0 bcc
Receive: 02 01 00 10 00 00 0f 5d 50 70 01 00 00 07 e0 01 01 3f 03 00 bcc

Example 2:
Read System Info of a Transponder without UID
Send: 02 01 02 02 21 2b bcc
Receive: 02 01 00 10 00 00 0f 5d 50 70 01 00 00 07 e0 01 01 3f 03 00 bcc

Note:
Please get the complete Coding of the flags from the **ISO/IEC 15693-3** Specification.
The block length read is one below then number of blocks in the transponder. So Block length 0x36 (63) means that the transponder has 0x40 (64) blocks.
The same is at the number of bytes per block. 0x03 (3) means 0x04 (4) Bytes per Block.

Commands for ISO15693 Transponder

7.21. Get multiple block security status

Data	Length	Meaning
1	**1**	ISO Request Flag
2	**1**	0x2c Get multiple block security status ISO Command
3 – 10	**8**	xxxx UID optional
3 or 11	**1**	xx Start block number
4 or 12	**1**	xx Block Length

Answer:

Data	Length	Meaning
1	**1**	Reader error
2	**1**	Response Flag
3 - n	**x**	**Block Security Status**

Example 1:
Read Block Security with Start block 15, Block Length 4 and with UID
Send: 02 01 20 0c 21 2c 5d 50 7a 01 00 00 07 e0 **0f 03** bcc
Receive: 02 01 00 06 00 00 01 00 00 01 bcc

Note:
The blocks at which the Bit 0 is set, in Block Security Status are **write protected**.
The Block Length is one below the actually read blocks.
This is as defined in the **ISO/IEC 15693-3** Specification.
At Block Length 0 one block is read, at Block Length 3 there are 4 Blocks read.

Commands for ISO15693 Transponder

7.22. ISO Write Data (only TS-HMK134 BT old devices)

The ISO Write Data Command is an extended command which does not show the communication with the chip directly as the ISO Raw Request command does, but uses a higher level of communication with the transponder programming device.
This command is used to write several successive blocks in the transponder.

CMD	Length	Data 1	Data 2- n
22h	n	Start block number	Block data

Start block number: Number of the Block which is the first to have data written to the transponder. Dependent on the transponder type different scopes are allowed.
Block Data: The length of the block data has to be a multiple of 4 because one block in the transponder always has 4 bytes. The length n is always a (multiple of 4) + 1!

Positive answer:

ERR	Length	Data
0	0	no Data

If a positive answer follows, this means the device has recognized the command. After programming of the transponder an additional answer follows. After this the command is finished and the next command can be send.
If the second answer is a positive answer, the transponder is successfully programmed. If it is a negative answer, the transponder could not be programmed.

If the first answer is a negative Answer, the command is finished with this answer.

7.23. ISO Check Status (only TS-HMK134 BT old devices)

The ISO Check Status command can be used to get the response state of the last ISO Write Data command.
The reason for the error can be read after the negative answer.

CMD	Length	Data
23h	0	no Data

Positive answer:

ERR	Length	Data 1
0	1	Status

Status: The error reason is bit coded:
Bit 0 = 1 No transponder found
Bit 1 = 1 Compare error at Read After Write

Commands for ISO14443-3 Transponder

8. Commands for ISO14443-3 (Mifare) Transponder

These commands are only supported at devices with write functionality and Mifare transponder support.
This can be derived from the device version.

8.1. Request

CMD	Length	Data 1
30h	1	Request Type

Request Type: Type of the Request
MIFARE_REQA (0x26) Activate only Transponders in Idle Mode
MIFARE_WUPA (0x52) Activate all Transponders
Alternatively the Request command can be used without Data (Length = 0), then MIFARE_REQA command is used.

Positive answer:

ERR	Length	Data 1 – n
0	2	Format of the available chips

Depending on the found Chips the supported modes are shown.
The Chip information of all found transponders are OR combined.

Commands for ISO14443-3 Transponder

8.2. Select

The select command has two variants

1. Select with Anti-collision, searches for a Transponder and selects this.

CMD	Length	Data
31h	0	no Data

The first found transponder is selected and the UID is returned. Hereby the different cascading levels are done automatically.

2. Select with defined UID

CMD	Length	Data 1-n
31h	n	UID

The transponder with the given UID is selected. The different cascading levels are selected automatically.
The length of the UID can be 4, 7 or 10 Bytes.

Positive answer (identically at both variants):

ERR	Length	Data 1	Data 2-n
0	n	SAK	UID of the found PICC

SAK — Select Acknowledge.
This confirms the selection of the transponder.
Meaning of the Bits at SAK:

B8	B7	B6	B5	B4	B3	B2	B1	Meaning
X	X	X	X	X	1	X	X	Cascading set, UID not complete
X	X	1	X	X	0	X	X	UID complete , compatible with ISO 14443-4
X	X	0	X	X	0	X	X	UID complete, not compatible with ISO 14443-3

The case 1 with B3=1 will never occur, because the cascading will be done inside of the reader completely.

Commands for ISO14443-3 Transponder

8.3. Halt

CMD	Length	Data
32h	0	no Data

The selected transponder (previously selected with Select) is halted.

Positive answer:

ERR	Length	Data
0	0	no Data

Transponder in HALT state can be activated by Select with UID or by Request with MIFARE_WUPA.

8.4. Authenticate Mifare Classic

There are different methods to do the Authentication of the Transponder.
- Authenticate with Key from E²PROM of the reader
- Authenticate with directly given Key
- Selection of the recently used Transponder
- Selection of the Transponders by UID

Authenticate without UID with Key from E²PROM

CMD	Length	Data 1	Data 2	Data 3	Data 4
33h	4	0	Block No.	Key Type	Address

Block Nr. Block number of the block to authenticate.
The complete sector where the block belongs to is authenticated.
Key Type Key type gives type of key and how to give the key
0=KeyA from E²Prom, 1=KeyB from E²Prom
Address Logical address in E²Prom where the Key is saved (0-15)

Authenticate with UID with Key from E²PROM

CMD	Length	Data 1	Data 2- 5	Data 6	Data 7	Data 8
33h	8	UID Length (4)	UID	Block No.	Key Type	Address

UID Length Length of UID (4 for Mifare classic)
UID UID of the Transponder
Block Nr. Block number of the block to authenticate.
The complete sector where the block belongs to is authenticated.
Key Type Key type gives type of key and how to give the key
0=KeyA from E²Prom, 1=KeyB from E²Prom
Address Logical address in E²Prom where the Key is saved (0-15)

Commands for ISO14443-3 Transponder

Authenticate without UID with Key directly given

CMD	Length	Data 1	Data 2	Data 3	Data 4-9
33h	9	0	Block No.	Key Type	Key

Block Nr. Block number of the block to authenticate.
The complete sector where the block belongs to is authenticated.
Key Type Key type gives type of key and how to give the key
2=KeyA directly given, 3=KeyB directly given.
Key 6 byte key information, LSB first

Authenticate with UID withKey directly given

CMD	Length	Data 1	Data 2- 5	Data 6	Data 7	Data 8-13
33h	13	UID Length (4)	UID	Block No.	Key Type	Key

UID Length Length of UID (4 for Mifare classic)
UID UID of the Transponder
Block Nr. Block number of the block to authenticate.
The complete sector where the block belongs to is authenticated.
Key Type Key type gives type of key and how to give the key
2=KeyA directly given, 3=KeyB directly given
Key 6 byte key information, LSB first

Positive answer:

ERR	Length	Data
0	0	no Data

Commands for ISO14443-3 Transponder

8.5. Write Key to E²Prom

CMD	Length	Data 1	Data 2	Data 3-8
39h	8	Key Type	Address	Key

Key Type — Key type gives type of key and how to give the key
0=KeyA, 1=KeyB

Address — Logical address in E²Prom where the Key is saved (0-15)

Key — 6 byte key information, LSB first

Positive answer:

ERR	Length	Data
0	0	no Data

Commands for ISO14443-3 Transponder

8.6. Read Block Mifare (Classic and Ultralight) resp. NFC

CMD	Length	Data 1
34h	1	Block number

Block number Number of the block, depends on Transponder

Positive answer:

ERR	Length	Data 1-16
0	16	Block Data

BlockData Data of the block, always 16 Byte.
At Mifare Ultralight and NFC Type 2 this returns always the content of 4 consecutive blocks beginning with the given block number.

8.7. Write Block Mifare (Classic and Ultralight) resp. NFC

CMD	Length	Data 1	Data 2- 17
35h	17	Block number	Block Data

Block number Number of the block, depends on Transponder
Block data Data of the block, always 16 Byte.

Positive answer:

ERR	Length	Data
0	0	no Data

Using Mifare Ultralight (NFC Type 2) always 4 Byte per Block are given, so the command is:

CMD	Length	Data 1	Data 2- 5
35h	5	Block number	Block Data

Block number Number of the block, depends on Transponder
Block data Data of the block, always 4 Byte.

Positive answer:

ERR	Length	Data
0	0	no Data

Commands for ISO14443-3 Transponder

8.8. Read value Mifare Classic

At transponders which support the value format, a "monetary value" can be saved.

CMD	Length	Data 1
36h	1	Block number

Block number Number of the block, depends on Transponder

Positive answer:

ERR	Length	Data 1 – 4
0	4	Value

Value Value, if valid value entry found, LSB first

8.9. Write value (Mifare Classic)

At transponders which support the value format, a "monetary value" can be saved.

CMD	Length	Data 1	Data 2- 5
37h	5	Block number	Value

Block number Number of the block, depends on Transponder
Value Value, LSB first

Positive answer:

ERR	Length	Data
0	0	no Data

8.10. Change Value (Mifare classic)

At transponders which support the value format, a "monetary value" can be saved.

CMD	Length	Data 1	Data 2	Data 3-6
38h	5	Block number	Direction	Value

Block number Number of the block, depends on Transponder
Direction Direction of change, 0 = Decrement, 1=Increment
Wert Amount to change, LSB first

Positive answer:

ERR	Length	Data
0	0	no Data

Commands for ISO14443-3 Transponder

8.11. Sector select Mifare Ultralight resp. NFC Type 2

At NFC Typ3 2 Transponder with more than 256 Blocks (more than 1024 Byte) to access the upper blocks, the appropriate sector has to be set.

CMD	Length	Data 1		
3Ah	1	Sector		

Sector Number of the sector, depends on the Transponder.

Positive answer:

ERR	Length	Data
0	0	no Data

8.12. Request, Wakeup ISO14443B

Determine whether an ISO14443B transponder is in the field

CMD	Length	Data 1	Data 2
3Bh	2	Type	AFI

Type 10Hex Request B
20Hex Wakeup B

AFI Application Family Identifier, see ISO 14443 Spec. Optional parameters. If not present, 0 is assumed.

Positive answer:

ERR	Length	Data 1-4	Data 5 – 8	Data 9 - 11
0	11	PUPI	AppData	ProtocolInfo

PUPI Pseudo Unique PICC Identifier, ID of the chip, unambiguous as long as it remains selected.

AppData Application data field see ISO14443 Spec.
Byte 1: AFI
Byte 2,3: CRC
Byte 4: Application number, LowNibble total, HighNibble for this AFI.

ProtocolInfo Byte 1: Supported bit rates, uplink and downlink, see ISO14443
Byte 2: Max. Frame size and protocol type, see ISO14443
Byte 3: Frame Wait Time und Options, see ISO14443

Commands for ISO14443-3 Transponder

8.13. Attrib ISO14443B

Send attributes for selection to the ISO14443B chip

CMD	Length	Data 1	Data 2 – 5
3Ch	5	Speed	PUPI

Speed — Transmission speed to be set.
Only the lowest 4 bits are valid,
2 bits each for PICC → PCD and PCD → PICC

Speed	PCD → PICC	PICC → PCD	Speed	PCD → PICC	PICC → PCD
0 (0000)	106 kBit	106 kBit	8 (1000)	106 kBit	424 kBit
1 (0001)	212 kBit	106 kBit	9 (1001)	212 kBit	424 kBit
2 (0010)	424 kBit	106 kBit	10 (1010)	424 kBit	424 kBit
3 (0011)	848 kBit	106 kBit	11 (1011)	848 kBit	424 kBit
4 (0100)	106 kBit	212 kBit	12 (1100)	106 kBit	848 kBit
5 (0101)	212 kBit	212 kBit	13 (1101)	212 kBit	848 kBit
6 (0110)	424 kBit	212 kBit	14 (1110)	424 kBit	848 kBit
7 (0111)	848 kBit	212 kBit	15 (1111)	848 kBit	848 kBit

PUPI — Pseudo Unique PICC Identifier, Chip ID with which the chip is addressed.
See also Request command.

Positive answer:

ERR	Length	Data
0	0	No Data

After activation of the chip with the Attrib command, the standard ISO14443 T = CL Transmit command can be accessed on the chip.

Commands for ISO14443-4 Transponder

9. Commands for ISO14443-4 (DesFire) Transponder

These commands are only available at devices which do have writing capabilities and support Mifare Desfire Transponder.
This can be derived from the device version.

9.1. ISO14443 SetPrologue

With this command the chip id is defined

CMD	Length	Data 1
40h	1	CID

CID Chip ID to talk to the chip.

Positive Answer:

ERR	Length	Data
0	0	no Data

9.2. ISO14443 RATS

Request for Answer to select command

CMD	Length	Data
41	0	No Data

Positive Answer:

ERR	Length	Data 1 – n
0	n	ATS

ATS “Answer to select” data as given in ISO 14443-4 resp. Desfire Documentation

Commands for ISO14443-4 Transponder

9.3. ISO14443 PPS

Protocol and Parameter Select

CMD	Length	Data 1
42	1	Speed

Speed Transmission speed,
only lower 4 Bit are valid,
2 Bits for PICC → PCD and PCD → PICC

Speed	PCD → PICC	PICC → PCD
0 (0000)	106 kBit	106 kBit
1 (0001)	212 kBit	106 kBit
2 (0010)	424 kBit	106 kBit
3 (0011)	848 kBit	106 kBit
4 (0100)	106 kBit	212 kBit
5 (0101)	212 kBit	212 kBit
6 (0110)	424 kBit	212 kBit
7 (0111)	848 kBit	212 kBit

Speed	PCD → PICC	PICC → PCD
8 (1000)	106 kBit	424 kBit
9 (1001)	212 kBit	424 kBit
10 (1010)	424 kBit	424 kBit
11 (1011)	848 kBit	424 kBit
12 (1100)	106 kBit	848 kBit
13 (1101)	212 kBit	848 kBit
14 (1110)	424 kBit	848 kBit
15 (1111)	848 kBit	848 kBit

Positive Answer:

ERR	Length	Data
0	0	no Data

Commands for ISO14443-4 Transponder

9.4. ISO14443 T=CL Transmit

The Transmit function is used to transmit all commands in T=CL command frame to the ISO14443 Chip. If the chip is set to encrypted data transfer, the encryption / decryption has to be done on host side, which means that data in the command is transferred encrypted.

CMD	Length	Data 1-n
45h	n	Data

Data data to be transmitted in T=CL command frame.

Positive Answer:

ERR	Length	Data 1 – n
0	n	Answer data in T=CL command frame
20h	n	Answer data in T=CL command frame

If ERR = 20h is returned, mode data is available which could not be transmitted in one step. (Chaining). Then using the following command “ISO14443 Chaining” the next data block is requested.

9.5. ISO14443 Chaining

With this the next data block is requested, if the previously transmitted command returned ERR = 20h announced more data.

CMD	Length	Data 1
46h	0	No data

Positive Answer:

ERR	Length	Data 1 – n
0	n	Answer data in T=CL command frame
20h	n	Answer data in T=CL command frame

At this command the announcement of an additional data block can be given by returning ERR = 20h.

Access to HF Reader IC

10. Commands to access the HF Reader IC

The following commands are only available at devices with appropriate HF Reader IC.
The TS-HRW38 uses the NXP CLRC632 and the TS-HRW32 the SIC9410 reader IC.

10.1. Read E²Prom of Controller IC

CMD	Length	Data 1-2	Data 3
05h	3	Start address	Length

Start address Start address in E²Prom, LSB first,
0x10: Start address MIFARE Register
0x30: Start address ISO15693 Register
0x50: Start address I.CODE Register
Length Number of bytes to be read from the E²Prom.

Positive answer:

ERR	Length	Data 1 – n
0	n	EEProm content

EEProm content data read from EEProm.

10.2. Write E²Prom of Controller IC

CMD	Length	Data 1-2	Data 3-n
06h	n	Start address	EEProm content

Start address Start address in E²Prom, LSB first,
0x10: Start address MIFARE Register
0x30: Start address ISO15693 Register
0x50: Start address I.CODE Register
EEProm content Data to be written to the E²Prom.
Using this, the standard parameters for the different modes can be changed.

Positive answer:

ERR	Length	Data
0	0	no Data

Access to HF Reader IC

10.3. Read Register of the Controller IC

CMD	Length	Data 1
07h	1	Register number

Register number Number of the Registers to be read

Positive answer:

ERR	Length	Data 1
0	1	Register content

Register content Content of the Register read

10.4. Write Register of the Controller IC

CMD	Length	Data 1	Data 2
08h	2	Register number	Register content

Register number Number of the Registers to be read
Register content Contents for the register

Positive answer:

ERR	Length	Data
0	0	no Data