iDTRONIC
PROFESSIONAL RFID

HF-RFID

Operation Notes

Issue 0.1
– 22. November 2023 –

Contents

1   General Information

1.1   Nomenclature

Telegrams from a PC or PLC to an RFID device: >>
Replies from an RFID device to a PC or PLC: <<

1.2   Glossary

RFU   Reserved for Future Use
UID   Unique IDentifier
VCD   Vicinity card device (RFID device)
VICC   Vicinity integrated circuit card (RFID data tag)

1.3   UID Output Sequence

For data tag types of the ISO14443A and ISO15693 standards, the output sequence is HEX-LSB-First according to the nomenclature.

For ISO14443A data tag types with 7 bytes UID, the manufacturer ID (for NXP: 0x04) is designated as LSB and is output after the size specification.

For ISO15693 data carrier types, the protocol identifier 0xE0 is designated as MSB in the ISO standard and is output at the end of the telegram.

The LSB is therefore always output first.

1.4   Manufacturer Identifiers

ISO14443A

There is no manufacturer identification for 4-byte long UIDs.
For 7-byte UIDs of ISO14443A data tags, the LSB is a manufacturer identifier.

Example: >> 50 00 02 22 10 26 46
              << 50 00 0B 22 44 00 08 07 04 49 69 AA 2B 2B 80 3C
07 = Length of the UID, which follows immediately
This is the UID: 04 49 69 AA 2B 2B 80
The 04 is the manufacturer identification.

ISO15693

The UID is always 8 bytes long. It has the protocol identifier E0 at one end and the manufacturer identifier close to it.

Example: >> 50 00 03 A1 26 00 00 D4
              << 50 00 08 A1 F5 25 26 9F 00 01 04 E0 75
This is the UID: F5 25 26 9F 00 01 04 E0
The 04 is the manufacturer ID and E0 is the protocol ID, which is always contained in the UID.

List of Manufacturers

01   Motorola (UK)
02   STMicroelectronics SA (FR)
03   Hitachi Ltd (JP)
04   NXP Semiconductors (DE)

05	Infineon Technologies AG (DE)
06	Cylink (US)
07	Texas Instruments (FR)
08	Fujitsu Limited (JP)
09	Matsushita Electronics Corporation, Semiconductor Company (JP)
0A	NEC (JP)
0B	Oki Electric Industry Co Ltd (JP)
0C	Toshiba Corp (JP)
0D	Mitsubishi Electric Corp (JP)
0E	Samsung Electronics Co Ltd (KR)
0F	Hynix (KR)
10	LG-Semiconductors Co Ltd (KR)
11	Emosyn-EM Microelectronics (US)
12	INSIDE Technology (FR)
13	ORGA Kartensysteme GmbH (DE)
14	Sharp Corporation (JP)
15	ATMEL (FR)
16	EM Microelectronic-Marin (CH)
17	SMARTRAC TECHNOLOGY GmbH (DE)
18	ZMD AG (DE)
19	XICOR Inc (US)
1A	Sony Corporation (JP)
1B	Malaysia Microelectronic Solutions Sdn Bhd (MY)
1C	Emosyn (US)
1D	Shanghai Fudan Microelectronics Co Ltd (CN)
1E	Magellan Technology Pty Limited (AU)
1F	Melexis NV BO (CH)
20	Renesas Technology Corp (JP)
21	TAGSYS (FR)
22	Transcore (US)
23	Shanghai Belling Corp Ltd (CN)
24	Masktech Germany GmbH (DE)
25	Innovision Research and Technology Plc (UK)
26	Hitachi ULSI Systems Co Ltd (JP)
27	Yubico AB (SE)
28	Ricoh (JP)
29	ASK (FR)
2A	Unicore Microsystems LLC (RU)
2B	Dallas semiconductor/Maxim (US)
2C	Impinj Inc (US)
2D	RightPlug Alliance (US)
2E	Broadcom Corporation (US)
2F	MStar Semiconductor Inc (TW)
30	BeeDar Technology Inc (US)
31	RFIDsec (DK)
32	Schweizer Electronic AG (DE)
33	AMIC Technology Corp (TW)
34	Mikron JSC (RU)
35	Fraunhofer Institute for Photonic Microsystems (DE)
36	IDS Microship AG (CH)

37	Kovio (US)
38	HMT Microelectronic Ltd (CH)
39	Silicon Craft Technology (TH)
3A	Advanced Film Device Inc. (JP)
3B	Nitecrest Ltd (UK)
3C	Verayo Inc. (US)
3D	HID Global (US)
3E	Productivity Engineering Gmbh (DE)
3F	Austriamicrosystems AG (reserved) (AT)
40	Gemalto SA (FR)
41	Renesas Electronics Corporation (JP)
42	3Alogics Inc (KR)
43	Top TroniQ Asia Limited (Hong Kong)
44	Gentag Inc (USA)
45	Invengo Information Technology Co.Ltd (CN)
46	Guangzhou Sysur Microelectronics, Inc (CN)
47	CEITEC S.A. (BR)
48	Shanghai Quanray Electronics Co. Ltd. (CN)
49	MediaTek Inc (TW)
4A	Angstrem PJSC (RU)
4B	Celisic Semiconductor (Hong Kong) Limited (CN)
4C	LEGIC Identsystems AG (CH)
4D	Balluff GmbH (DE)
4E	Oberthur Technologies (FR)
4F	Silterra Malaysia Sdn. Bhd. (MY)
50	DELTA Danish Electronics, Light & Acoustics (DK)
51	Giesecke & Devrient GmbH (DE)
52	Shenzhen China Vision Microelectronics Co., Ltd. (CN)
53	Shanghai Feiju Microelectronics Co. Ltd. (CN)
54	Intel Corporation (US)
55	Microsensys GmbH (DE)
56	Sonix Technology Co., Ltd. (TW)
57	Qualcomm Technologies Inc (US)
58	Realtek Semiconductor Corp (TW)
59	Freevision Technologies Co. Ltd (CN)
5A	Giantec Semiconductor Inc. (CN)
5B	JSC Angstrem-T (RU)
5C	STARCHIP France
5D	SPIRTECH (FR)
5E	GANTNER Electronic GmbH (AT)
5F	Nordic Semiconductor (NO)
60	Verisiti Inc (US)
61	Wearlinks Technology Inc. (CN)
62	Userstar Information Systems Co., Ltd (TW)
63	Pragmatic Printing Ltd. (UK)
64	Associação do Laboratório de Sistemas Integráveis Tecnológico – LSI-TEC (BR)
65	Tendyron Corporation (CN)
66	MUTO Smart Co., Ltd.(KR)
67	ON Semiconductor (US)
68	TÜBİTAK BİLGEM (TR)

69   Huada Semiconductor Co., Ltd (CN)
6A   SEVENEY (FR)
6B   ISSM (FR)
6C   Wisesec Ltd (IL)
7E   Holtek (TW)

Source: https://www.kartenbezogene-identifier.de/de/chiphersteller-kennungen.html

2   Manufacturer-specific Commands

2.1   Notes for Data Tags of Type ISO1443A

As the successor to the Mifare Ultralight, the NTAG family offers additional functions, including a FAST_READ with which the entire memory can be read in one go. There is no direct support for these functions in the firmware of the RFID device, but the transfer command with the command code 0x2E can call up these and future functions of the data carrier.

The information in brackets refers to the manufacturer data sheets of the NTAG family.

Start Communication with PICCActivate

>> 50 00 02 22 10 26 46
<< 50 00 0B 22 44 00 00 07 04 F0 A8 82 59 49 80 74

GET_VERSION (Chapter 10.1 page 34)

>> 50 00 01 2E 60 1F
<< 50 00 08 2E 00 04 04 02 01 00 0F 03 79

READ_SIG (Chapter 10.8 page 47)

>> 50 00 02 2E 3C 00 40
<< 50 00 20 2E 6E 91 3A 0D 85 90 65 78 77 07 7D 11 F7 2F 14 84 55 36 C9 20 1C 83 32 1B 9F 96 6C 42 6C FD 5F 23 3C

PWD_AUTH (Chapter 10.7 page 46)

>> 50 00 05 2E 1B 00 00 00 00 60 – wrong password…
<< F0 00 01 2E 01 DE – … results in the error message

>> 50 00 05 2E 1B FF FF FF FF 60 – now with correct password
<< 50 00 02 2E 00 00 7C

FAST_READ (Chapter 10.3 page 23)

>> 50 00 03 2E 3A 00 06 41
50   = Start of Telegram
00 03   = Data Length
2E   = Command Byte, PICCTransfer
    3A   = FAST_READ
    00   = Number of the first memory page to be read
    06   = Number of the last memory page to be read
41   = Checksum

You will then receive a rather long telegram in response, which may look like this
50   = Start of Telegram
00 1C   = Data Length
2E   = Command Byte
04 73 06 F9   = first memory page
11 BF 61 80   = second memory page
4F 48 00 00   = third memory page
E1 10 3E 00   = fourth memory page
03 16 D1 01   = fifth memory page
55 55 55 55   = sixth memory page
66 66 66 66   = seventh memory page
A8   = Checksum

2.2   Notes for Data Tags of Type ISO 15693

The ST25DV64KC chip type offers a read/write memory of 8 kBytes. The standard read/write command is based on the ISO standard and therefore only has one address byte. This means that only 256 × 4 = 1024 bytes can be addressed, or 256 × 8 = 2 kByte with the 8-byte blocks of the Fujitsu MB89R118.

The ST25DV64KC therefore has additional manufacturer-specific commands. Although these are not directly supported by the firmware, they can be used with the PICCTransfer command (0x2E). These extended read/write commands are described in chapters "7.6.13 Extended Read Multiple Blocks" and "7.6.15 Extended Write Multiple Blocks" as well as "7.6.40 Fast Extended Read Multiple Block" in the chip manufacturer's data sheet.

Firstly, communication is opened with I2_Inventory (0xA1). Then the command PICCTransfer (0x2E) is used for the data tag-specific special functions.

1. Manufacturer Specific Tag Command "Fast Extended Read Multiple Blocks"

SOF   is automatically prefixed by the firmware, so omit it

40	Flags
C5	Command Fast Extended Read Multiple Blocks
02	Mfg code

UID is not to be sent depending on the flags. The address bit is not set for flags 0x40, so no UID needs to be sent.

00 00	Start block
01 23	End block 292

CRC16 is calculated by the firmware, so omit it
EOF is automatically added by the firmware, so omit it

2. Insert Tag Command into PICCTransfer

>> 50 00 07 2E 40 C5 02 00 00 01 23 DC

50	Start of Telegram
00 07	7 Bytes Payload
2E	Command Byte, PICCTransfer
40 C5 02 00 00 01 23	The data to be sent to the RFID data tag
DC	BCC

Note

Please note that the communication protocol only allows a payload of 506 bytes!

3   Notes for Data Tags of Type ISO15693

3.1   Flags

ISO15693 has a byte with flags that are used for every communication.
The flag for addressed communication and the options flag for some data tag types are important.

3.1.1 Flags 1 bis 4

Bit #	Flag Name	Value	Description
1	Sub-carrier_flag	0	A single sub-carrier frequency shall be used by the data tag.
		1	Two sub-carrier frequency shall be used by the data tag.
2	Data_rate_flag	0	Low data rate shall be used.
		1	High data rate shall be used.
3	Inventory_flag	0	Flags 5 to 8 meaning is according to table "Flags 5 to 8, Standard"
		1	Flags 5 to 8 meaning is according to table "Flags 5 bis 8, Inventory"
4	ProtocolExtension_flag	0	No protocol format extension.
		1	Protocol format is extended. Reserved for future use.

3.1.2 Flags 5 to 8, Standard

Bit #	Flag Name	Value	Description
5	Select_flag	0	Request shall be executed by any VICC according to the setting of Address_flag.
		1	Request shall be executed only by VICC in selected state.
6	Address_flag	0	Request is not addressed. UID field is not present. It shall be executed by any VICC.
		1	Request is addressed. UID field is present. It shall be executed only by the VICC whose UID matches the UID specified in the request.
7	Option_flag	0	Meaning is defined by the command description. It shall be set to 0 if not otherwise defined by the command.*
		1	Meaning is defined by the command description.*
8	RFU	0	RFU, shall be set to 0.

* Handling may vary depending on the data tag type and manufacturer. Information on this can be found in the manufacturer's data sheet.

3.1.3 Flags 5 to 8, Inventory

Bit #	Flag Name	Value	Description
5	AFI_flag	0	AFI field is not present
		1	AFI field is present
6	Nb_slots_flag	0	16 slots
		1	1 slots
7	Option_flag	0	Meaning is defined by the command description. It shall be set to 0 if not otherwise defined by the command.*
		1	Meaning is defined by the command description.*
8	RFU	0	RFU, shall be set to 0.

* Handling may vary depending on the data tag type and manufacturer. Information on this can be found in the manufacturer's data sheet.

3.2   Options Flags

Even if the chip manufacturers base their optional command codes on the ISO15693 standard, there may be special features. For example, some chips expect the options flag to be set when writing. This is the case, for example, with the Tag-it family from Texas Instruments:

Table 1-1. Command Set for Tag-it HF-I Plus Transponder

REQUEST	REQUEST CODE	REQUEST MODE (1)					
		INVENTORY	ADDRESSED	NON-ADDRESSED	Select	AFI	OPT. FLAG
ISO 15693 Mandatory Commands							
Inventory	0x01	✓	–	–	–	✓	0
Stay Quiet	0x02	–	✓	–	–	–	0
ISO 15693 Optional Commands							
Read_Single_Block	0x20	✓	✓	✓	✓	✓	0/1
Write_Single_Block	0x21	–	✓	✓	✓	–	1
Lock_Block	0x22	–	✓	✓	✓	–	1
Read_Multi_Blocks	0x23	✓	✓	✓	✓	✓	0/1
Select Tag	0x25	–	✓	–	–	–	0
Reset to Ready	0x26	–	✓	✓	✓	–	0
Write_AFI	0x27	–	✓	✓	✓	–	1
Lock_AFI	0x28	–	✓	✓	✓	–	1
Write DSFID	0x29	–	✓	✓	✓	–	1
Lock DSFID	0x2A	–	✓	✓	✓	–	1
Get_System_info	0x2B	✓	✓	✓	✓	✓	0
Get_M_Blk_Sec_St	0x2C	✓	✓	✓	✓	✓	0
TI Custom Commands							
Write_2_Blocks	0xA2	–	✓	✓	✓	–	1
Lock_2_Blocks	0xA3	–	✓	✓	✓	–	1

(1)   ✓: Implemented
       –: Not applicable
       0/1: Option flag needed

NOTE: The Option Flag (Bit 7) of the ISO 15693 defined Request Flags must be set to 1 for all Write and Lock commands to respond properly.

Source: Tag-it HF-I Plus TMS37112 Reference Guide (2010-04), SCBU004B

3.3   Typical Values of the Flag Byte

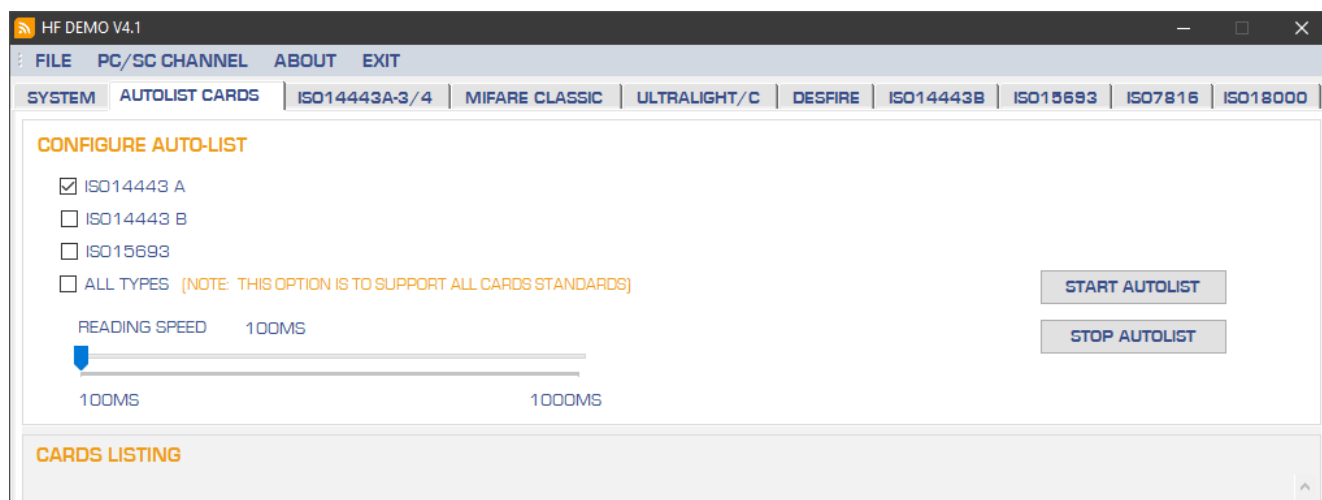| Flags	Description
0x02	High speed, no UID required (no addressed mode)
0x22	High speed, UID must be specified (addressed mode)
0x42	High speed, no UID required (no addressed mode), option flag = 1
0x62	High speed, UID must be specified (addressed mode), option flag = 1

4   Auto-List Function in the Demo-Software

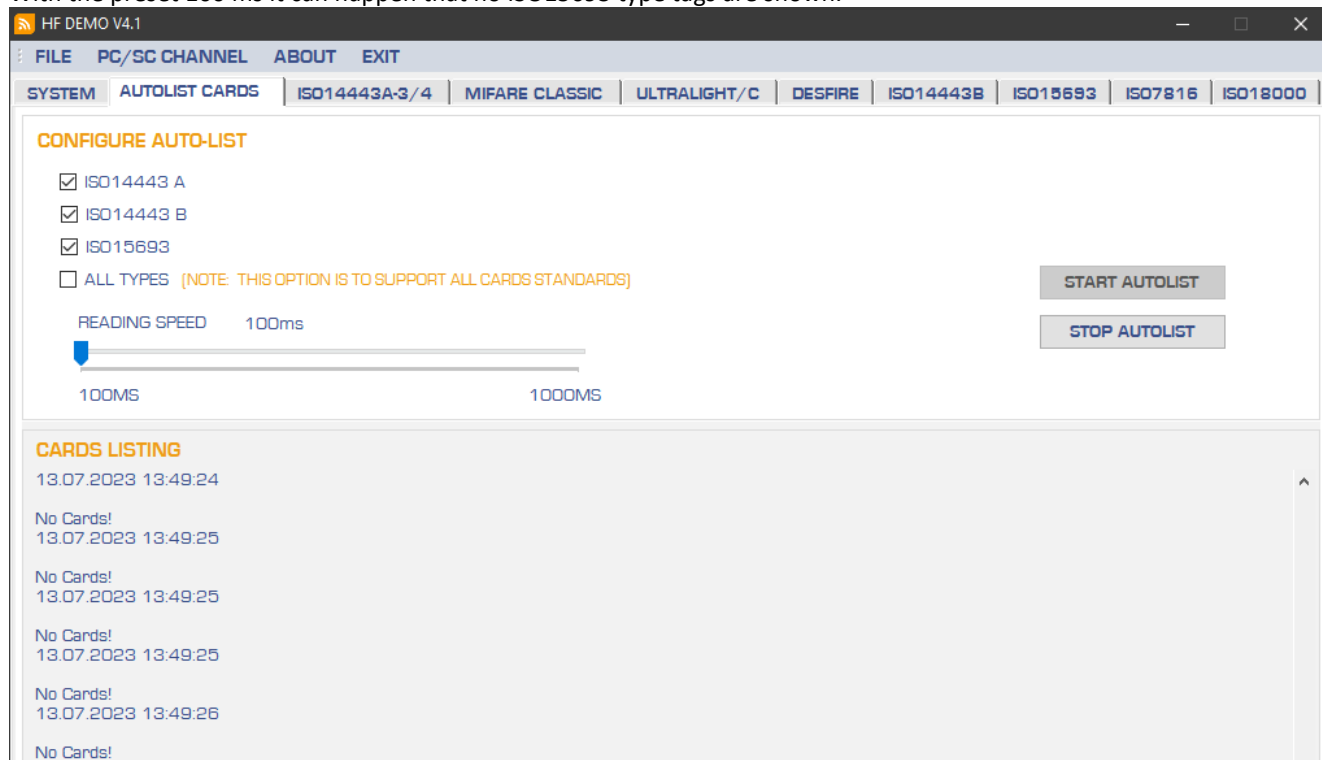This tab is to send continuous commands to detect tags. Use this tab to detect the tag type.

This is not a configuration tab for the explicit auto-list cards configuration command 0x23.
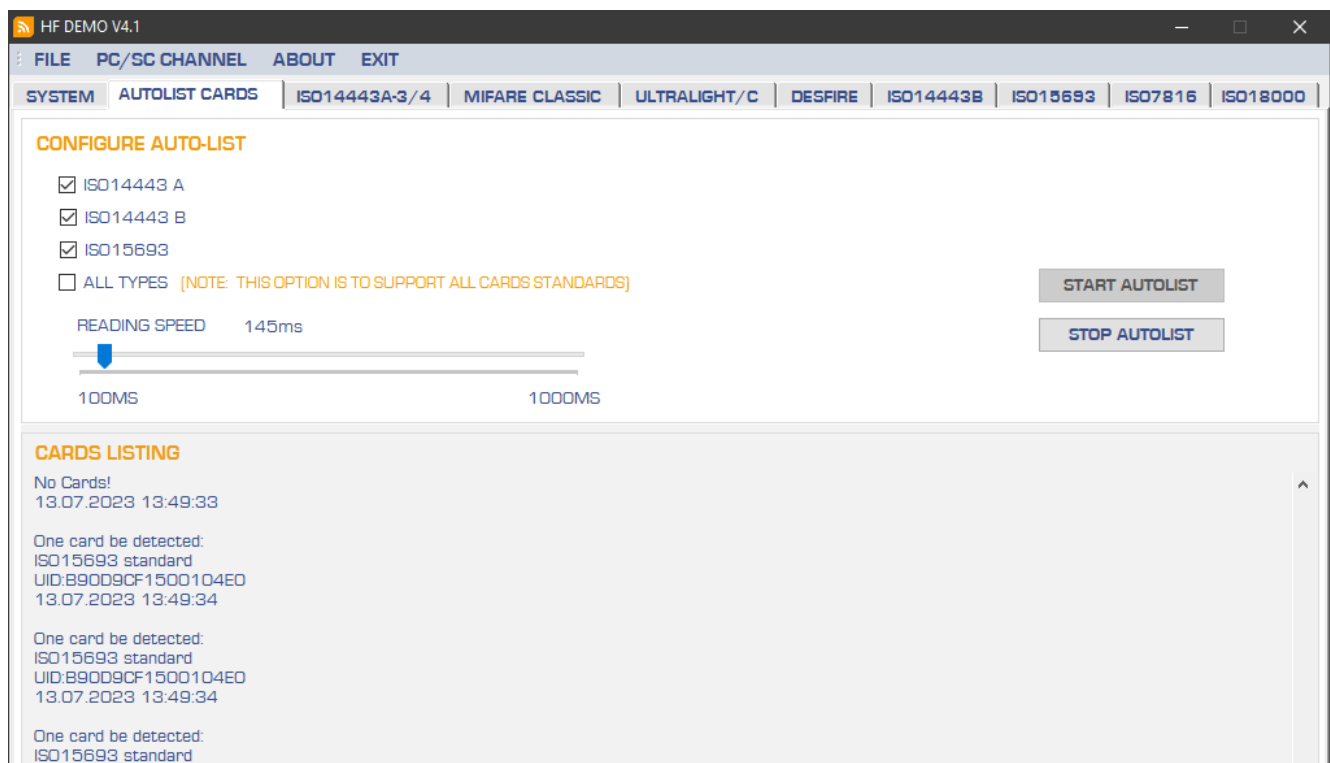
The test software uses this commands:

For ISO14443A:	50 00 02 22 10 26 46	request idle
For ISO14443B:	50 00 04 41 00 00 00 00 15	
For ISO15693:	50 00 03 A1 26 00 00 D4	single slot inventory

With the preset 100 ms it can happen that no ISO15693 type tags are shown.

Please enlarge the reading speed to more than 150 ms for successful detection of ISO 15693 type tags:

5   Revisions

Version	Date	Notes
0.1	2023-11-22	First Issue