Research and Production Enterprise "DISC SYSTEMS" LTD
EDRPOU 16303375, a/c No.260075014037759
at PJSC "UKREXIMBANK" in c. Kyiv
MFO 380333, TIN 163033726585

03061, Ukraine, c. Kyiv, 95-S Otradny ave., Telephone +372 880 78 78. Fax +38044 507 02 02. www.bitrek.eu, sales@bitrek.eu

Operating Manual

Module
BI CONNECT MF01

Version 2019.12.1

www.bitrek.eu
sales@bitrek.eu
+372 880 78 78

Contents

Purpose of the device

The BI CONNECT MF01 module of BITREK CONNECT system is a card reader for MIFARE® Classic 1K cards and is intended for identification, work shift logging, fuel fill up control, etc. A number of a card and its status read by the module are transmitted to CONNECT-BUS and can be used by other modules of the BITREK CONNECT system.

Scope of delivery

The scope of delivery of BI CONNECT MF01 module for the BITREK CONNECT system is as follows:

- Module BI CONNECT MF01 – 1 pc.
- Technical datasheet – 1 pc.
- Warranty certificate – 1 pc.
- Package box– 1 pc.

Device specifications

Device specifications are shown in Table 1 below.

Table 1. Device specifications

No.	Parameters	Characteristics
1	Input voltage	12/24 V
2	Current consumption (12 V)	30 mA
3	Interface	RS-485, CAN (CONNECT BUS)
4	Data exchange protocol for RS-485	SOVA
5	Operating frequency	13.56 MHz
6	Proximity cards type	MIFARE® Classic 1K
7	Max. size of proximity cards (W × L × H)	86 x 54 x 1.5 mm
8	Max. number of cards stored to memory	1 million
9	Operating temperature range	-30 °C to +80 °C
10	Relative humidity	80 % ± 15 %
11	Dimensions (W × L × H)	85 × 105 × 30 mm
12	Net weight	300 g
13	Gross weight	340 g
14	Housing protection class	IP67

Appearance of the device and its dimensions

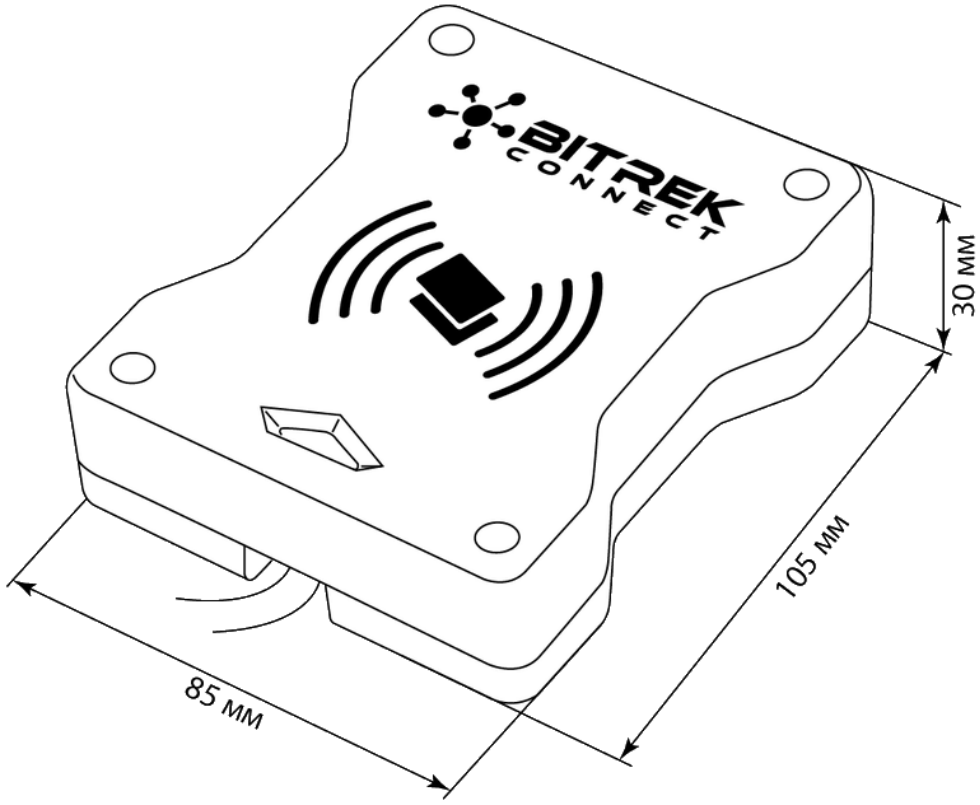

Figure 1. Appearance and dimensions

Device pin assignment

Purpose of output terminals of BI CONNECT MF01 is shown in Table 2.

Table 2. Purpose of device contacts

No.	Contact name	Signal type	Color	Contact assignment
1	+Vin	Power supply	White	"+" onboard power supply (rated voltage 12 V or 24 V)
2	GND	Power supply	Grey	Common cable (ground)
3	CAN-H	Input/ output	Pink	Signal "H" CAN interface
4	CAN-L	Input/ output	Brown	Signal "L" CAN interface
5	«A» RS-485	Input/ output	Yellow	Signal "A" RS-485 interface
6	«B» RS-485	Input/ output	Green	Signal "B" RS-485 interface

Indication description

The front panel of the module has a LED indicator that indicates current status of the device.

Table 3. LED indication

LED state	Description
Red	The device is connected to power
Yellow	A MIFARE® card is brought to the device, the card cannot be authorized
Green	An authorized MIFARE® card is brought to the device
Blinking	More than one card is attached to the device – cards cannot be read

Module operation algorithm

The BI CONNECT MF01 module of the BITREK CONNECT system is compatible with MIFARE® Classic 1K cards.

The device can operate in two modes.

Secure mode is the major mode of device operation. In this mode, the device and a card exchange data using ciphering algorithm. To operate in this mode, the MIFARE® cards have to be pre-programmed using a special procedure. The procedure is described in the respective section of this document. Besides, to access a card in the secure mode, a card reading key is used that is unique to a group of programmed cards. The reading key is programmed to the reader and the cards cannot be read without it.

This mode can be used when MF01 is used with cards that will not be used in other systems simultaneously.

Insecure mode is a simplified mode, in which MF01 reads UID of a card chip only. In this mode, cards are read without using a ciphering algorithm. The data recorded to the card memory are not read, only UID of a card is read. When operating in the insecure mode, obtained card UIDs cannot be stored to the device memory.

This mode can be useful when operating with the respective ciphered cards or cards that have been locked earlier and are used in other systems or in a pre-access system.

The mode is selected by setting the value of the ID_Conf 0300 parameter. This parameter may be set with 2 values: 0 – 'card read key' corresponding to the secure mode, and 2 – 'the key is disabled' corresponding to the insecure mode. Secure mode requires a ciphering key, which is configured in parameter ID_Conf 0920.

When the MF01 reader is active in the secure mode, it may perform card validation. The reader has its own memory that may store up to 1 million cards. Depending on the validity of the cards, the reader sends a respective status to Connect-Bus – '*Own card*' card in case of a card that has been found in the memory of the device, or 'Foreign card' in case the reader fails to find the card in the memory. In both cases, however, card number will be sent to Connect-Bus. When RS-485 is used, only card number is transmitted. Validity attribute is not transmitted in this case. Apart from the status sent to the bus, LED on the front panel of the device also indicates the validity of the proximity card. Refer to the respective section of this Manual for more details about the LED indication.

Configuring BI CONNECT MF01

BI CONNECT MF01 has several configurable parameters listed in Appendix 1. To configure the BI CONNECT MF01 module, a BITREK CONNECT system configurator is used along with CONNECT Configurator software. The procedure of operation of the configurator and use of the software is detailed in *Manual for Setting Up and Configuration of BITREK CONNECT System*.

The module can store up to 1 million card numbers to the memory. The commands in Table 4 below are used to operate the memory of the device.

Table 4. List of commands for operation of BI CONNECT MF01

No.	Command	Description
1	setparam ####	Set a parameter value by its ID
2	getparam ####	Get a parameter value by its ID
3	saveparam	Save the parameters to FLASH
4	addekey	Add an electronic key
5	clearekey	Blocking an electronic key
6	matchekey	Search a key number in the memory
7	formatekey	Remove all keys from the memory
8	getver	Device firmware version request

Explanation to Table 4:

Set a parameter value by its ID/get a parameter value by its ID.

Standard commands for reading and writing the parameters. The list of all configurable parameters is given in Appendix 1.

Save parameters to FLASH.

After each change of the settings, the following command needs to be sent to the module: *saveparam*

Once the module receives the command, it responds as follows: *"PARAM SAVED"* and saves modified parameters to FLASH memory.

Add an electronic key.

Example of the command:
addekey XXXXXXXXXX;

where:
addekey – command;
XXXXXXXXXX – ID of an electronic key, 10 characters sharp.
The device responds with the result of saving and result code.
The following response are possible:
"addekey: OK,0" – the key has been saved successfully;
"addekey: MATCH,0" – a key match has been found;
"addekey: ERR,0" – the system has failed to save the key due to incorrect ID;
"addekey: ERR,1" – entry format error (card number does not consist of 10 characters; unacceptable characters are used).

Clear an electronic key.

This command is used for clearing an ID of an electronic key from the device memory. A cleared key cannot be unlocked but it can be added as a new key using the *addekey* command.

Example of the command:
clearekey XXXXXXXXXX;

where:
clearekey – command;
XXXXXXXXXX – ID of an electronic key.

The following responses are possible:
"clearekey: OK,0" – the key has been successfully cleared from the memory;
"clearekey: ERR,0" – error during command execution;

Search for a key in the memory.

The command is used for searching keys in the device memory.

Example of the command:
matchekey XXXXXXXXXX;

where:
matchekey – command;
XXXXXXXXXX – ID of an electronic key.
The system responds with the search result and result code.
The following responses are possible:
"matchekey: OK,0" – the key has been found in the memory;
"matchekey: ERR,0" – the key has not been found in the memory.

Remove all numbers of electronic keys from the memory.

The command is used to erase all electronic keys from the memory.

Example of the command:
formatekey;

The system returns the following response:
"formatekey: OK" – the command has been executed successfully.

Get software version.

This command is used for getting a string with software version.

Example of the command:
getver;

The system returns the following response:
"VER: MF01 V1 0005 19"

MIFARE® card recording procedure

The module MF01, the module CAN of Bitrek Connect system configurator and Mifare® Writer program for Windows are used for programming cards.

The sequence of actions when connecting equipment:

1. Connect the MF01 module to the CAN module of the configurator. The connection is made via CAN bus; in this case, it is necessary to provide terminator resistor between the signal lines CAN H and CAN L at the level of 60 - 120 Ohm.
2. Connect the CAN configurator to the computer via USB interface.
3. Power up the MF01 module.

Description of the program MIFARE® Writer.

The view of the program window is shown in Fig.2.

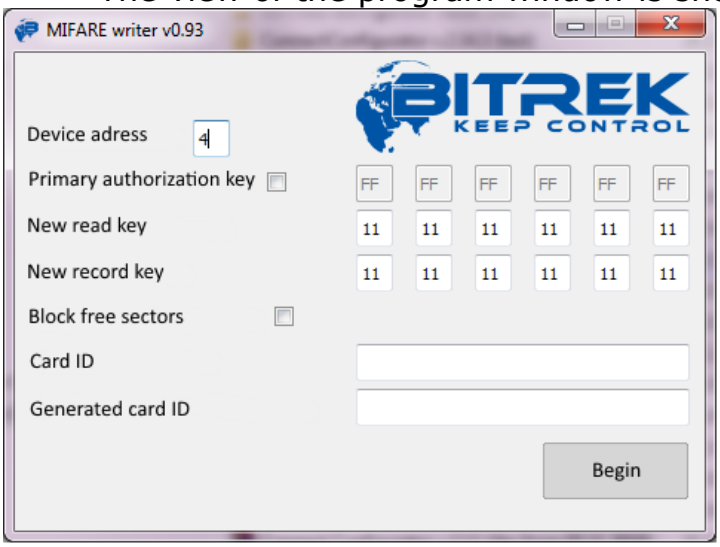

Figure 2. MIFARE® Writer software

Device address - is the address of the MF01 module on the CAN bus. The default is 4.
Primary authorization key - is a key that is used to re-record cards that were previously recorded. It's not used when working with a new card.
New read key - is the key that will be used to read the card after recording.
New record key - is the key that will be used to re-record the card, if necessary.
Block free sectors - blocking free sectors of the memory card.
Card ID - is the ID of the card, which is entered by the user and on the basis of which the final card number will be calculated. The possible values for this field are 1 - 999999.
Generated card ID - is a field unavailable for data entry. This field will display the generated final card number, which will be transmitted by the MF01 module when reading this card. The generated final number must be saved immediately after the card is recorded and associated to the newly recorded card.

Procedure for programming new cards that were not previously in operation

1. The Primary Authorization Key is not used to program a new card - this field is not necessary.
2. In the "New Read Key" field, you need to enter the key that will be used to read the card data. Further, in order to read the cards recorded with this Read Key, it will be necessary to write this key using the Connect Configurator program into the corresponding parameter of the MF01 module (the parameter id is 0920, the parameter name is the "Card Read Key").
3. In the "New Record Key" field, you need to enter a key, which you can later use to re-record the card.

4. In the “Card ID” field, you need to enter a number on the basis of which the system will generate the final card number. The possible values for this field are 1 - 999999.
5. After entering all the parameters, you need to click the button “Begin” and put a new card into the reader. If everything was done correctly, the card will be programmed, the final identifier key will be generated and entered into the appropriate field, and the program will show the notification of successful recording.

The generated identifier key must be saved and then associated with the number marked on the card (if available) for the convenience of operation with the cards.

Important!
The program does not keep logs and statistics. Therefore, all used keys and generated numbers should be saved in any convenient way before the next recording procedure.

Procedure for re-programming cards that were previously recorded

1. To reprogram the cards that were previously recorded, you need to check a toolbox “Primary Authorization Key”, after which the field for entering this key will become available. In this field you need to enter the key which during the previous programming was indicated as “New Record Key”.
2. In the "New Read Key" field you need to enter the key that will be used to read the card data. Further, in order to read the cards recorded with this Read Key, it will be necessary to write this key using the Connect Configurator program into the corresponding parameter of the MF01 module (the parameter id is 0920, the parameter name is the “Card Read Key”).
3. In the "New Record Key" field, you need to enter a key, which you can use to re-record the card.
4. In the “Card ID” field, you need to enter a number on the basis of which the system will generate the final card number.
5. After entering all the parameters, you need to click the button “Begin” and put a new card into the reader. If everything was done correctly, the card will be programmed, the final identifier key will be generated and entered into the appropriate field and the program will show the notification of successful recording.

When programming the card, the information is recorded into the Sector No. 4. After recording, all other sectors can be locked for recording. In case a new card is programmed that will not be used in other systems, it is recommended to block free sectors. This will increase the reliability of information security. In case the card will be used in other systems, it is not necessary to block free sectors, but recording to the used Sector No. 4 will be impossible.

The generated final identifier will be transmitted to the Connect-Bus bus and via the RS-485 interface upon request. You can also use this identifier when recording a card to the device’s memory.

List of variables transmitted to the CONNECT-BUS

No.	Parameter name	Bit depth	PGN	Start Bit	Bit Total	Timeout
1	Device model	4	18F713	0	32	10
2	Software version	4	18F713	32	32	10
3	Module operation time	4	18F712	0	32	10
4	Number of module restarts	4	18F712	32	32	10
5	Card status	1	18F701	0	8	5
6	Card number	8	18F701	16	40	5

Note:
The variable "Card Status" can take on the values:
01 - card is not detected;
03 - card is detected, but not authorized, the status is "Foreign card";
07 - card is detected and authorized, the status is "Own card".

Appendix 1. Device parameters

No.	Parameter name	Configuration ID	Bit depth	Description	Default value
General					
1	CANSlaveAddr	0200	1 byte	Device address on the CONNECTBUS	4
2	RS485Addr	0201	1 byte	Device address on the RS-485	9
3	DeviceName	0510	1 byte	Full name of the device	MIFARE READER REV001
Periods					
4	CANSendPeriod	0700	2 bytes	Period of sending the main data packet via CAN (msec)	1001
5	CANWaitPeriod	0701	1 byte	The holding period of valid data by CAN (sec)	1
MIFARE settings					
6	EkeyPrio	0300	1 byte	Key priority 0 - card reading key (secure mode); 2 - key is not used (insecure mode)	0
7	EkeyRead	0920	6 bytes	Card reading key	FFFFFFFFFFFF
Security					
8	DevicePIN	0910	1 byte	Terminal password to access the device	11111

Document version

Date	Revision	Note
25/03/2019	2019.03.1	Primary document
28/03/2019	2019.03.2	Description of programming cards was expanded, technical characteristics were exceeded
18/12/2019	2019.12.1	Minor technical characteristics of the device were added, card recording procedure was clarified