



OEM-DES-RFID-Lock
13.56 MHz OEM RFID Lock with CAN-Bus
Teach-In Example

iDTRONIC GmbH
Ludwig-Reichling-Straße 4
67059 Ludwigshafen
Germany/Deutschland

Phone: +49 621 6690094-0
Fax: +49 621 6690094-9
E-Mail: info@idtronic.de
Web: idtronic.de

Issue 0.2
– 28. February 2023 –

Subject to alteration without prior notice.
© Copyright iDTRONIC GmbH 2023
Printed in Germany

Contents

1	General.....	4
1.1	Introduction	4
1.2	Reading out the FW of the CAN controller.....	4
1.3	Reading out the FW of the RFID module.....	4
2	Settings for RFID Tag Access	5
2.1	Set 3DES Key	5
2.2	Set ApplicationNr	5
2.3	Set Application KeyNr.....	6
2.4	Set Application Key	6
2.5	Set Flags with File Information	6
2.6	Set FileNr.....	7
2.7	Set KeyNr for File Access	7
2.8	Key für Dateizugriff setzen	7
3	After the Settings	8
3.1	Write File, new RFID key is created	8
3.2	Read File, existing RFID key is read.....	8

1 General

1.1 Introduction

In the following there is communication between 2 partners:

Configuration Software and RFID Lock: 1BC00036 <> 1BC1B000

RFID Lock and ECU_A: 1BC1B001 <> 1BC00836 (found in the final chapter)

1.2 Reading out the FW of the CAN controller

#	Address	Contents	Function
1	1BC00036	03 22 60 41 AA AA AA AA	0 = Single Frame 3 = 3 Bytes of payload follow 22 = Read by Identifier 60 41 = Command Code The following are padding bytes
2	1BC1B000	10 22 62 60 41 44 45 53	First Frame with Contents 44 45 53 = DES
3	1BC00036	30 0F 00	Flow Control: up to 15 blocks allowed, breaks unnecessary
4	1BC1B000	21 2D 4C 4F 43 4B 2D 43	Consecutive Frame with Contents 2D 4C 4F 43 4B 2D 43 = -LOCK-C
5	1BC1B000	22 41 4E 2D 4B 45 20 56	Consecutive Frame with Contents 41 4E 2D 4B 45 20 56 = AN-KE V
6	1BC1B000	23 32 30 20 32 30 32 31	Consecutive Frame with Contents 32 30 20 32 30 32 31 = 20 2021
7	1BC1B000	24 30 37 32 33 20 50 4D	Consecutive Frame with Contents 30 37 32 33 20 50 4D = 0723 PM
8	1BC1B000	25 00 00 00 00 00 00 00	Consecutive Frame with Closing Character 00

1.3 Reading out the FW of the RFID module

#	Address	Contents	Function
1	1BC00036	03 22 60 42 AA AA AA AA	0 = Single Frame 3 = 3 Bytes of payload follow 22 = Read by Identifier 60 42 = Command Code The following are padding bytes
2	1BC1B000	10 25 62 60 42 4F 45 4D	First Frame with Contents 4F 45 4D = OEM
3	1BC00036	30 0F 00	Flow Control: up to 15 blocks allowed, breaks unnecessary
4	1BC1B000	21 2D 44 45 53 2D 4D 38	Consecutive Frame with Contents 2D 44 45 53 2D 4D 38 = -DES-M8
5	1BC1B000	22 39 30 2D 54 54 4C 20	Consecutive Frame with Contents 39 30 2D 54 54 4C 20 = 90-TTL
6	1BC1B000	23 32 30 32 30 30 36 30	Consecutive Frame with Contents 32 30 32 30 30 36 30 = 2020060
7	1BC1B000	24 31 20 31 31 3A 34 32	Consecutive Frame with Contents 31 20 31 31 3A 34 32 = 1 11:42
8	1BC1B000	25 20 41 4D 00 00 00 00	Consecutive Frame with Contents 20 41 4D 00 = AM

2 Settings for RFID Tag Access

2.1 Set 3DES Key

#	Address	Contents	Function
1	1BC00036	10 1B 2E 60 31 AF 70 6A	First Frame Telegram 01B = 27 Bytes of payload follow 2E = Write Data by identifier 60 31 = Send 3DES Key AF 70 6A
2	1BC1B000	30 00 0A	Flow Control: no restriction on the number of blocks, 10 ms pause
3	1BC00036	21 24 3F 71 7E 4B 7D 2A	Consecutive Frame with Contents
4	1BC00036	22 5E 8B 3B 35 38 32 5A	Consecutive Frame with Contents
5	1BC00036	23 2D 73 D3 97 5D 78 6D	Consecutive Frame with Contents
6	1BC1B000	03 6E 60 31	Confirmation from RFID lock

3DES Key: AF706A243F717E4B7D2A5E8B3B3538325A2D73D3975D786D

Important Note

After that, the parameter part of the payload is encrypted. The commands remain unencrypted.

2.2 Set ApplicationNr

#	Address	Contents	Function
1	1BC00036	10 0B 2E 60 02 C0 F5 09	First Frame Telegram 00B = 11 Bytes of payload follow 2E = Write Data by identifier 60 02 = Send AppNr
2	1BC1B000	30 00 0A	Flow Control: no restriction on the number of blocks, 10 ms pause
3	1BC00036	21 80 23 CD C3 5F AA AA	Consecutive Frame with Contents
4	1BC1B000	03 6E 60 02	Confirmation from RFID lock

C0 F5 09 80 23 CD C3 5F is application number ED CB A9

Encrypted

DES????

???

MAC??

XOR??

????

??

???

DES(???)

3DES(???)

3DES(???)

??

Key (24 Bytes)

AF706A243F717E4B7D2A5E8B3B3538325A2D73D3975D786D

48

??

Data (8 bytes)

C0F5098023CDC35F

16

??

Result (8 Bytes)

EDCBA9B9E1D90F83

Encrypt

Decrypt

??

??

☐ ???

OEM RFID Modules

Page 5 of 8

2.3 Set Application KeyNr

#	Address	Contents	Function
1	1BC00036	10 0B 2E 60 03 1B 27 A7	First Frame Telegram 00B = 11 Bytes of payload follow 2E = Write Data by identifier 60 03 = Send KeyNr
2	1BC1B000	30 00 0A	Flow Control: no restriction on the number of blocks, 10 ms pause
3	1BC00036	21 0D 7C 5B 11 8D AA AA	Consecutive Frame with Contents
4	1BC1B000	03 6E 60 03	Confirmation from RFID lock

1B 27 A7 0D 7C 5B 11 8D is key number 00

2.4 Set Application Key

#	Address	Contents	Function
1	1BC00036	10 13 2E 60 04 5F FE 9D	First Frame Telegram 013 = 19 Bytes of payload follow 2E = Write Data by identifier 60 04 = Send Key
2	1BC1B000	30 00 0A	Flow Control: no restriction on the number of blocks, 10 ms pause
3	1BC00036	21 40 02 0E 79 5A EC 1E	Consecutive Frame with Contents
4	1BC00036	22 D0 2D 6B 26 CA B0 AA	Consecutive Frame with Contents
5	1BC1B000	03 6E 60 04	Confirmation from RFID lock

5F FE 9D 40 02 0E 79 5A EC 1E D0 2D 6B 26 CA B0 is key value 760B470545394C0B405F3D3D3457745A (16 Bytes)

2.5 Set Flags with File Information

#	Address	Contents	Function
1	1BC00036	10 0B 2E 60 11 51 A9 53	First Frame Telegram 00B = Bytes of payload follow 2E = Write Data by identifier 60 03 = Send KeyNr
2	1BC1B000	30 00 0A	Flow Control: no restriction on the number of blocks, 10 ms pause
3	1BC00036	21 A1 95 E1 14 0A AA AA	Consecutive Frame with Contents
4	1BC1B000	03 6E 60 11	Confirmation from RFID lock

51 A9 53 A1 95 E1 14 0A contains the information 00 00 10 10 00

2.6 Set FileNr

#	Address	Contents	Function
1	1BC00036	10 0B 2E 60 12 C9 DC A3	First Frame Telegram 00B = 11 Bytes of payload follow 2E = Write Data by identifier 60 12 = Send FileNr
2	1BC1B000	30 00 0A	Flow Control: no restriction on the number of blocks, 10 ms pause
3	1BC00036	21 E3 B8 72 61 A9 AA AA	Consecutive Frame with Contents
4	1BC1B000	03 6E 60 12	Confirmation from RFID lock

C9 DC A3 E3 B8 72 61 A9 is file number 04

2.7 Set KeyNr for File Access

#	Address	Contents	Function
1	1BC00036	10 0B 2E 60 13 52 AC 39	First Frame Telegram 00B = 11 Bytes of payload follow 2E = Write Data by identifier 60 13 = Send KeyNr
2	1BC1B000	30 00 0A	Flow Control: no restriction on the number of blocks, 10 ms pause
3	1BC00036	21 87 8A 92 C8 A0 AA AA	Consecutive Frame with Contents
4	1BC1B000	03 6E 60 13	Confirmation from RFID lock

52 AC 39 87 8A 92 C8 A0 is key number 01.

2.8 Key für Dateizugriff setzen

#	Address	Contents	Function
1	1BC00036	10 13 2E 60 14 05 7E F3	First Frame Telegram 013 = 19 Bytes of payload follow 2E = Write Data by identifier 60 14 = Send Key
2	1BC1B000	30 00 0A	Flow Control: no restriction on the number of blocks, 10 ms pause
3	1BC00036	21 20 6C 6B D5 EE 8A 74	Consecutive Frame with Contents
4	1BC00036	22 73 E6 79 08 72 E4 AA	Consecutive Frame with Contents
5	1BC1B000	03 6E 60 14	Confirmation from RFID lock

05 7E F3 20 6C 6B D5 EE 8A 74 73 E6 79 08 72 E4 is the key value 5075254A26530F354A5866324234464D

3 After the Settings

3.1 Write File, new RFID key is created

#	Address	Contents	Function
1	1BC00036	10 0B 2E 60 21 4C 71 38	First Frame Telegram 00B = 11 Bytes of payload follow 2E = Write Data by identifier 60 21 = Write File
2	1BC1B000	30 00 0A	Flow Control: no restriction on the number of blocks, 10 ms pause
3	1BC00036	21 B6 58 0C 74 16 AA AA	Consecutive Frame with Contents
4	1BC1B000	03 6E 60 21	Confirmation from RFID lock

4C 71 38 B6 58 0C 74 16 contains 4 Bytes with contents 11223344

Important Note

Immediately after this new RFID key is taught, it is recorded and the file content is reported to the ECU_A:

3.2 Read File, existing RFID key is read

#	Address	Contents	Function
1	0600	No Contents	ECU_A Wakeup, then 400 ms waiting time
2	0600	No Contents	ECU_A Wakeup, then immediately Read File, sent from the RFID lock
3	1BC1B001	10 0B 62 60 22 88 0C 95	RFID lock sends Read File First Frame 00B = 11 Bytes of payload follow 62 = Read Data by identifier, SID erhöht um 40 60 22 = Read File
4	1BC00836	30 03 0A	Flow Control
5	1BC1B001	21 40 B6 25 2B FA 00 00	Consecutive Frame with Contents

88 0C 95 40 B6 25 2B FA contain 4 bytes from the file with the contents 11223344