



**OEM-DES-RFID-Lock**  
**13.56 MHz OEM RFID-Schloss mit CAN-Bus**  
**Teach-In-Beispiel**

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

Ausgabe 0.2  
– 28. Februar 2023 –

Phone: +49 621 6690094-0  
Fax: +49 621 6690094-9  
E-Mail: [info@idtronic.de](mailto:info@idtronic.de)  
Web: [idtronic.de](http://idtronic.de)

Änderungen ohne vorherige Ankündigung vorbehalten.  
© Copyright iDTRONIC GmbH 2023  
Printed in Germany

## Inhalt

<b>1</b>	<b>Allgemein .....</b>	<b>4</b>
1.1	Einführung.....	4
1.2	Auslesen der FW des CAN-Controllers .....	4
1.3	Auslesen der FW der RFID-Baugruppe .....	4
<b>2</b>	<b>Einstellungen für den RFID-Datenträgerzugriff .....</b>	<b>5</b>
2.1	3DES Key setzen .....	5
2.2	ApplicationNr einstellen .....	5
2.3	Application KeyNr einstellen .....	6
2.4	Application Key setzen .....	6
2.5	Flags mit Dateinformationen setzen .....	6
2.6	FileNr setzen.....	7
2.7	KeyNr für Dateizugriff setzen.....	7
2.8	Key für Dateizugriff setzen .....	7
<b>3</b>	<b>Nach dem Einstellen .....</b>	<b>8</b>
3.1	Write File, neuer RFID-Schlüssel wird erstellt .....	8
3.2	Read File, vorhandener RFID-Schlüssel wird erfasst .....	8

# 1 Allgemein

## 1.1 Einführung

Im Folgenden gibt es die Kommunikation zwischen 2 Partnern:

Einstellsoftware und RFID-Schloss: 1BC00036 <> 1BC1B000

RFID-Schloss und ECU\_A: 1BC1B001 <> 1BC00836 (im letzten Kapitel zu finden)

## 1.2 Auslesen der FW des CAN-Controllers

#	Adresse	Inhalt	Funktion
1	1BC00036	03 22 60 41 AA AA AA AA	0 = Single Frame 3 = es folgen 3 Bytes Nutzlast 22 = Read by Identifier 60 41 = Kommandokode Es folgen Füllbytes
2	1BC1B000	10 22 62 60 41 44 45 53	First Frame mit Inhalt 44 45 53 = DES
3	1BC00036	30 0F 00	Flow Control: bis zu 15 Blöcke erlaubt, Pausen unnötig
4	1BC1B000	21 2D 4C 4F 43 4B 2D 43	Consecutive Frame mit Inhalt 2D 4C 4F 43 4B 2D 43 = -LOCK-C
5	1BC1B000	22 41 4E 2D 4B 45 20 56	Consecutive Frame mit Inhalt 41 4E 2D 4B 45 20 56 = AN-KE V
6	1BC1B000	23 32 30 20 32 30 32 31	Consecutive Frame mit Inhalt 32 30 20 32 30 32 31 = 20 2021
7	1BC1B000	24 30 37 32 33 20 50 4D	Consecutive Frame mit Inhalt 30 37 32 33 20 50 4D = 0723 PM
8	1BC1B000	25 00 00 00 00 00 00 00	Consecutive Frame mit Schlusszeichen 00

## 1.3 Auslesen der FW der RFID-Baugruppe

#	Adresse	Inhalt	Funktion
1	1BC00036	03 22 60 42 AA AA AA AA	0 = Single Frame 3 = es folgen Bytes Nutzlast 22 = Read by Identifier 60 42 = Kommandokode Es folgen Füllbytes
2	1BC1B000	10 25 62 60 42 4F 45 4D	First Frame mit Inhalt 4F 45 4D = OEM
3	1BC00036	30 0F 00	Flow Control: bis zu 15 Blöcke erlaubt, Pausen unnötig
4	1BC1B000	21 2D 44 45 53 2D 4D 38	Consecutive Frame mit Inhalt 2D 44 45 53 2D 4D 38 = -DES-M8
5	1BC1B000	22 39 30 2D 54 54 4C 20	Consecutive Frame mit Inhalt 39 30 2D 54 54 4C 20 = 90-TTL
6	1BC1B000	23 32 30 32 30 30 36 30	Consecutive Frame mit Inhalt 32 30 32 30 30 36 30 = 2020060
7	1BC1B000	24 31 20 31 31 3A 34 32	Consecutive Frame mit Inhalt 31 20 31 31 3A 34 32 = 1 11:42
8	1BC1B000	25 20 41 4D 00 00 00 00	Consecutive Frame mit Inhalt 20 41 4D 00 = AM

## 2 Einstellungen für den RFID-Datenträgerzugriff

### 2.1 3DES Key setzen

#	Adresse	Inhalt	Funktion
1	1BC00036	10 1B 2E 60 31 AF 70 6A	First Frame Telegramm 01B = es folgen 27 Bytes Nutzlast 2E = Write Data by identifier 60 31 = Send 3DES Key <b>AF 70 6A</b>
2	1BC1B000	30 00 0A	Flow Control: keine Einschränkung bei der Blockzahl, 10 ms Pause
3	1BC00036	21 <b>24 3F 71 7E 4B 7D 2A</b>	Consecutive Frame mit Inhalt
4	1BC00036	22 <b>5E 8B 3B 35 38 32 5A</b>	Consecutive Frame mit Inhalt
5	1BC00036	23 <b>2D 73 D3 97 5D 78 6D</b>	Consecutive Frame mit Inhalt
6	1BC1B000	03 6E 60 31	Bestätigung vom RFID-Schloss

3DES-Schlüssel: **AF706A243F717E4B7D2A5E8B3B3538325A2D73D3975D786D**

#### Wichtiger Hinweis

Danach wird der Parameterteil der Nutzlast verschlüsselt. Die Kommandos bleiben unverschlüsselt.

### 2.2 ApplicationNr einstellen

#	Adresse	Inhalt	Funktion
1	1BC00036	10 0B 2E 60 02 <b>C0 F5 09</b>	First Frame Telegramm 00B = es folgen 11 Bytes Nutzlast 2E = Write Data by identifier 60 02 = Send AppNr
2	1BC1B000	30 00 0A	Flow Control: keine Einschränkung bei der Blockzahl, 10 ms Pause
3	1BC00036	21 <b>80 23 CD C3 5F</b> AA AA	Consecutive Frame mit Inhalt
4	1BC1B000	03 6E 60 02	Bestätigung vom RFID-Schloss

**C0 F5 09 80 23 CD C3 5F** ist die Applikations-Nummer ED CB A9

#### Entschlüsselt

DES????

??? | MAC?? | XOR?? | ???? | ??

???  
☐ DES(???)  
☐ 3DES(???)  
☒ 3DES(???)

**Key (24 Bytes)**  
 AF706A243F717E4B7D2A5E8B3B3538325A2D73D3975D786D 48

**Data (8 bytes)**  
 C0F5098023CDC35F 16

**Result (8 Bytes)**  
 EDCBA9B9E1D90F33

Encrypt ?? Decrypt ??

☐ ????

## 2.3 Application KeyNr einstellen

#	Adresse	Inhalt	Funktion
1	1BC00036	10 0B 2E 60 03 <b>1B 27 A7</b>	First Frame Telegramm 00B = es folgen 11 Bytes Nutzlast 2E = Write Data by identifier 60 03 = Send KeyNr
2	1BC1B000	30 00 0A	Flow Control: keine Einschränkung bei der Blockzahl, 10 ms Pause
3	1BC00036	21 <b>0D 7C 5B 11 8D</b> AA AA	Consecutive Frame mit Inhalt
4	1BC1B000	03 6E 60 03	Bestätigung vom RFID-Schloss

**1B 27 A7 0D 7C 5B 11 8D** ist die Key-nummer 00

## 2.4 Application Key setzen

#	Adresse	Inhalt	Funktion
1	1BC00036	10 13 2E 60 04 <b>5F FE 9D</b>	First Frame Telegramm 013 = es folgen 19 Bytes Nutzlast 2E = Write Data by identifier 60 04 = Send Key
2	1BC1B000	30 00 0A	Flow Control: keine Einschränkung bei der Blockzahl, 10 ms Pause
3	1BC00036	21 <b>40 02 0E 79 5A EC 1E</b>	Consecutive Frame mit Inhalt
4	1BC00036	22 <b>D0 2D 6B 26 CA B0</b> AA	Consecutive Frame mit Inhalt
5	1BC1B000	03 6E 60 04	Bestätigung vom RFID-Schloss

**5F FE 9D 40 02 0E 79 5A EC 1E D0 2D 6B 26 CA B0** ist der Key 760B470545394C0B405F3D3D3457745A (16 Bytes)

## 2.5 Flags mit Dateiinformatioren setzen

#	Adresse	Inhalt	Funktion
1	1BC00036	10 0B 2E 60 11 <b>51 A9 53</b>	First Frame Telegramm 00B = es folgen 11 Bytes Nutzlast 2E = Write Data by identifier 60 03 = Send KeyNr
2	1BC1B000	30 00 0A	Flow Control: keine Einschränkung bei der Blockzahl, 10 ms Pause
3	1BC00036	21 <b>A1 95 E1 14 0A</b> AA AA	Consecutive Frame mit Inhalt
4	1BC1B000	03 6E 60 11	Bestätigung vom RFID-Schloss

**51 A9 53 A1 95 E1 14 0A** enthält die Information 00 00 10 10 00

## 2.6 FileNr setzen

#	Adresse	Inhalt	Funktion
1	1BC00036	10 0B 2E 60 12 C9 DC A3	First Frame Telegramm 00B = es folgen 11 Bytes Nutzlast 2E = Write Data by identifier 60 12 = Send FileNr
2	1BC1B000	30 00 0A	Flow Control: keine Einschränkung bei der Blockzahl, 10 ms Pause
3	1BC00036	21 E3 B8 72 61 A9 AA AA	Consecutive Frame mit Inhalt
4	1BC1B000	03 6E 60 12	Bestätigung vom RFID-Schloss

C9 DC A3 E3 B8 72 61 A9 ist die Dateinummer 04

## 2.7 KeyNr für Dateizugriff setzen

#	Adresse	Inhalt	Funktion
1	1BC00036	10 0B 2E 60 13 52 AC 39	First Frame Telegramm 00B = es folgen 11 Bytes Nutzlast 2E = Write Data by identifier 60 13 = Send KeyNr
2	1BC1B000	30 00 0A	Flow Control: keine Einschränkung bei der Blockzahl, 10 ms Pause
3	1BC00036	21 87 8A 92 C8 A0 AA AA	Consecutive Frame mit Inhalt
4	1BC1B000	03 6E 60 13	Bestätigung vom RFID-Schloss

52 AC 39 87 8A 92 C8 A0 ist die Dateinummer 01.

## 2.8 Key für Dateizugriff setzen

#	Adresse	Inhalt	Funktion
1	1BC00036	10 13 2E 60 14 05 7E F3	First Frame Telegramm 013 = es folgen 19 Bytes Nutzlast 2E = Write Data by identifier 60 14 = Send Key
2	1BC1B000	30 00 0A	Flow Control: keine Einschränkung bei der Blockzahl, 10 ms Pause
3	1BC00036	21 20 6C 6B D5 EE 8A 74	Consecutive Frame mit Inhalt
4	1BC00036	22 73 E6 79 08 72 E4 AA	Consecutive Frame mit Inhalt
5	1BC1B000	03 6E 60 14	Bestätigung vom RFID-Schloss

05 7E F3 20 6C 6B D5 EE 8A 74 73 E6 79 08 72 E4 ist der Key 5075254A26530F354A5866324234464D

### 3 Nach dem Einstellen

#### 3.1 Write File, neuer RFID-Schlüssel wird erstellt

#	Adresse	Inhalt	Funktion
1	1BC00036	10 0B 2E 60 21 4C 71 38	First Frame Telegramm 00B = es folgen 11 Bytes Nutzlast 2E = Write Data by identifier 60 21 = Write File
2	1BC1B000	30 00 0A	Flow Control: keine Einschränkung bei der Blockzahl, 10 ms Pause
3	1BC00036	21 B6 58 0C 74 16 AA AA	Consecutive Frame mit Inhalt
4	1BC1B000	03 6E 60 21	Bestätigung vom RFID-Schloss

4C 71 38 B6 58 0C 74 16 enthält 4 Bytes Dateiinhalt 11223344

#### Wichtiger Hinweis

Sofort nach dem Einlernen dieses neuen RFID-Schlüssels wird dieser erfasst und der Dateiinhalt zur ECU\_A gemeldet:

#### 3.2 Read File, vorhandener RFID-Schlüssel wird erfasst

#	Adresse	Inhalt	Funktion
1	0600	Kein Inhalt	ECU_A Wakeup, danach 400 ms Wartezeit
2	0600	Kein Inhalt	ECU_A Wakeup, danach sofort Read File, gesendet vom RFID-Schloss
3	1BC1B001	10 0B 62 60 22 88 0C 95	RFID-Schloss sendet Read File First Frame 00B = es folgen 11 Bytes Nutzlast 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 mit Inhalt

88 0C 95 40 B6 25 2B FA enthalten 4 Bytes aus der Datei mit dem Inhalt 11223344