

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  Phone: +49 621 6690094-0  Fax: +49 621 6690094-9  E-Mail: info@idtronic.de  Web: idtronic.de | Issue 0.1  – 08. Dezember 2022 –  Subject to alteration without prior notice.  © Copyright iDTRONIC GmbH 2022  Printed in Germany |

Contents

[1 Allgemein 4](#_Toc121412613)

[1.1 Einführung 4](#_Toc121412614)

[1.2 Auslesen der FW des CAN-Controllers 4](#_Toc121412615)

[1.3 Auslesen der FW der RFID-Baugruppe 4](#_Toc121412616)

[2 Einstellungen für den RFID-Datenträgerzugriff 5](#_Toc121412617)

[2.1 3DES Key setzen 5](#_Toc121412618)

[2.2 ApplicationNr einstellen 5](#_Toc121412619)

[2.3 Application KeyNr einstellen 6](#_Toc121412620)

[2.4 Application Key setzen 6](#_Toc121412621)

[2.5 Flags mit Dateiinformationen setzen 6](#_Toc121412622)

[2.6 FileNr setzen 7](#_Toc121412623)

[2.7 KeyNr für Dateizugriff setzen 7](#_Toc121412624)

[2.8 Key für Dateizugriff setzen 7](#_Toc121412625)

[3 Nach dem Einstellen 8](#_Toc121412626)

[3.1 Write File, neuer RFID-Schlüssel wird erstellt 8](#_Toc121412627)

[3.2 Read File, vorhandener RFID-Schlüssel wird erfasst 8](#_Toc121412628)

# Allgemein

## 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)

## 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 Identifyer  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 |

## 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 Identifyer  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 |

# Einstellungen für den RFID-Datenträgerzugriff

## 3DES Key setzen

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

3DES-Schlüssel: AF706A243F717E4B7D2A5E8B3B3538325A2D73D3975D786D

Wichtiger Hinweis

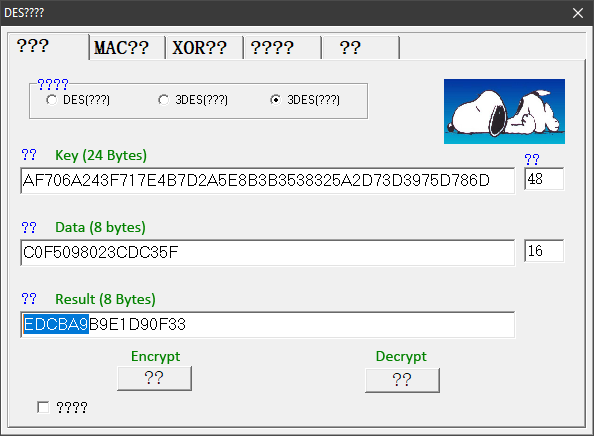
Danach wird der Parameterteil der Nutzlast verschlüsselt. Die Kommandos bleiben unverschlüsselt.

## ApplicationNr einstellen

|  |  |  |  |
| --- | --- | --- | --- |
| # | Adresse | Inhalt | Funktion |
| 1 | 1BC00036 | 10 0B 2E 60 02 C0 F5 09 | First Frame mit 3DES-Schlüssel  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 80 23 CD C3 5F 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



## Application KeyNr einstellen

|  |  |  |  |
| --- | --- | --- | --- |
| # | Adresse | Inhalt | Funktion |
| 1 | 1BC00036 | 10 0B 2E 60 03 1B 27 A7 | First Frame mit 3DES-Schlüssel  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 0D 7C 5B 11 8D AA AA | Consecutive Frame mit Inhalt |
| 4 | 1BC1B000 | 03 6E 60 03 | Bestätigung vom RFID-Schloss |

1B 27 A70D 7C 5B 11 8D ist die Key-nummer 00

## Application Key setzen

|  |  |  |  |
| --- | --- | --- | --- |
| # | Adresse | Inhalt | Funktion |
| 1 | 1BC00036 | 10 13 2E 60 04 5F FE 9D | First Frame mit 3DES-Schlüssel  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 40 02 0E 79 5A EC 1E | Consecutive Frame mit Inhalt |
| 4 | 1BC00036 | 22 D0 2D 6B 26 CA B0 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)

## Flags mit Dateiinformationen setzen

|  |  |  |  |
| --- | --- | --- | --- |
| # | Adresse | Inhalt | Funktion |
| 1 | 1BC00036 | 10 0B 2E 60 11 51 A9 53 | First Frame mit 3DES-Schlüssel  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 A1 95 E1 14 0A 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

## FileNr setzen

|  |  |  |  |
| --- | --- | --- | --- |
| # | Adresse | Inhalt | Funktion |
| 1 | 1BC00036 | 10 0B 2E 60 12 C9 DC A3 | First Frame mit 3DES-Schlüssel  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

## KeyNr für Dateizugriff setzen

|  |  |  |  |
| --- | --- | --- | --- |
| # | Adresse | Inhalt | Funktion |
| 1 | 1BC00036 | 10 0B 2E 60 13 52 AC 39 | First Frame mit 3DES-Schlüssel  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.

## Key für Dateizugriff setzen

|  |  |  |  |
| --- | --- | --- | --- |
| # | Adresse | Inhalt | Funktion |
| 1 | 1BC00036 | 10 13 2E 60 14 05 7E F3 | First Frame mit 3DES-Schlüssel  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

# Nach dem Einstellen

## Write File, neuer RFID-Schlüssel wird erstellt

|  |  |  |  |
| --- | --- | --- | --- |
| # | Adresse | Inhalt | Funktion |
| 1 | 1BC00036 | 10 0B 2E 60 21 4C 71 38 | First Frame mit 3DES-Schlüssel  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 Dateinhalt zur ECU\_A gemeldet:

## 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