

# 13.10.2020 // DESFire Protokoll

## LibLogicalAccess

“Müssen wir uns mal anschauen, da die das können, was wir wollen

## Links

- [KeySettings](#)
- [MIFARE DESFire EV2 Datasheet](#)
- [MIFARE DESFire EV1 Datasheet](#)
- [Phillips DesFire Tool Manual](#)
- [DesFire for Python Docs](#)
- [DesFire for Python Code](#)
- [MIFARE ISO/IEC 14443 Spec](#)
- [Ridrix DesFire Commands](#)
- [DesFire Missing Native Commands Forum](#)
- [ISO 7816-4](#)
- [MIFARE DESFire as Type 4 Tag](#)
- [ISO/IEC7816-4](#)
- [MIFARE DESFire Short Spec](#)
- [libfreefare](#)
- [DesFire Proof-of-Concept](#)
- [DesFire Client](#)
- [DesFire Server](#)
- [DesFire Application Bytes](#)
- [DesFire Java App](#)
- [DesFire Arduino Project](#)
- [Kommunikationsbeispiele](#)

- [\*\*DESFire Lib from JavaCardOS\*\*](#)
- DESFire Commands sind nur unter NDA verfügbar.
- [DESFire EV2 Error Code Forum](#)
- [Response Codes](#)
- [Mifare DESFire Application](#)
- [DESFire Authentication](#)
- [DESFire Light Authentication Mifare Spec](#)
- [Phillips DESFire Training](#)
- [Mifare Application Dir](#)
- [DESFire Door Lock](#)
- [DESFire Auth 2K3DES](#)
- [Easypay DESFire Lib](#) - sehr brauchbar

## Bytes

### APDU Commands

- SELECT = 00 a4 04 00 07 d2 76 00 00 85 01 00 00
- VERSION = 90 60 00 00 00
- CONTINUE = 90 AF 00 00 00

### APDU Responses

APDU responses will first contain the data followed by two status bytes.

- FRAME\_CONTINUE = 91 AF
- OPERATION\_OK = 91 00
- OK = 90 00
- INIT = ??
- VERSION 1 = 04 01 01 01 00 1a 05
- VERSION 2 = 04 01 01 01 03 1a 05
- VERSION 3 = 04 91 3a 29 93 26 80 00 00 00 00 39 08

### Instructions DESFire (used inside ADPU)

CLA = 0x90 APDU Struktur -> ISO/IEC 7816-4 Befehle -> DESFire

- 0x0A = AUTHENTICATE
- 0x1A = AUTHENTICATE\_ISO
- 0xAA = AUTHENTICATE\_AES
- 0x71 = AUTHENTICATE\_EV2\_FIRST (EV2 only)
- 0x77 = AUTHENTICATE\_EV2\_NONFIRST (EV2 only)
- 0x54 = CHANGE\_KEY\_SETTINGS
- 0x5C = SET\_CONFIGURATION
- 0xC4 = CHANGE\_KEY
- 0x?? = CHANGE\_KEY\_EV2 (EV2 only)
- 0x?? = INITIALIZE\_KEY\_SET (EV2 only)
- 0x?? = FINALIZE\_KEY\_SET (EV2 only)
- 0x?? = ROLL\_KEY\_SET (EV2 only)
- 0x64 = GET\_KEY\_VERSION
- 0xCA = CREATE\_APPLICATION
- 0x?? = CREATE\_DELEGATE\_APPLICATION (EV2 only)
- 0xDA = DELETE\_APPLICATION
- 0x6A = GET\_APPLICATION\_IDS
- 0x6E = FREE\_MEMORY
- 0x6D = GET\_DF\_NAMES
- 0x?? = GET\_DELEGATE\_INFO (EV2 only)
- 0x45 = GET\_KEY\_SETTINGS
- 0x5A = SELECT\_APPLICATION
- 0xFC = FORMAT\_PICC
- 0x60 = GET\_VERSION
- 0x51 = GET\_CARD\_UID
- 0x6F = GET\_FILE\_IDS
- 0xF5 = GET\_FILE\_SETTINGS
- 0x5F = CHANGE\_FILE\_SETTINGS
- 0xCD = CREATE\_STDDATAFILE
- 0xCB = CREATE\_BACKUPDATAFILE
- 0xCC = CREATE\_VALUE\_FILE
- 0xC1 = CREATE\_LINEAR\_RECORD\_FILE
- 0xC0 = CREATE\_CYCLIC\_RECORD\_FILE
- 0x?? = CREATE\_TRANSACTION\_MAC\_FILE (EV2 only)
- 0xDF = DELETE\_FILE
- 0x61 = GET\_ISO\_FILE\_IDS
- 0xBD = READ\_DATA (manchmal auch als 0x8D beschrieben)
- 0x3D = WRITE\_DATA
- 0x6C = GET\_VALUE
- 0x0C = CREDIT
- 0xDC = DEBIT

- 0x1C = LIMITED\_CREDIT
- 0x3B = WRITE\_RECORD
- 0xBB = READ\_RECORDS
- 0xEB = CLEAR\_RECORD\_FILE
- 0x?? = UPDATE\_RECORD\_FILE
- 0xC7 = COMMIT\_TRANSACTION
- 0xA7 = ABORT\_TRANSACTION
- 0xAF = CONTINUE
- 0x?? = COMMIT\_READER\_ID (EV2 only)

## Instructions ISO/IEC 7816-4 (nativ, aber von DESFire unterstützt)

CLA = 0x00 APDU Sturuktur -> ISO/IEC 7816-4 Befehle -> ISO/IEC 7816-4

- 0xA4 = SELECT FILE
- 0xB0 = READ BINARY
- 0xD6 = UPDATE BINARY
- 0xB2 = READ RECORDS
- 0xE2 = APPEND RECORD
- 0x84 = GET CHALLENGE
- 0x88 = INTERNAL AUTHENTICATE
- 0x82 = EXTERNAL AUTHENTICATE

## Instruction ISO 14443-3

### Status Codes

from <https://github.com/JavaCardOS/pyResMan/blob/master/pyResMan/DESFireEx.py#L54>  
 which, has it from <https://github.com/jekkos/android-hce-desfire/blob/master/hceappletdesfire/src/main/java/net/jpeelaer/hce/desfire/DesfireStatusWord.java>

- 0x00 = OPERATION\_OK Successful operation
- 0x0C = NO\_CHANGES No changes done to backup files, CommitTransaction / AbortTransaction not necessary
- 0x0E = OUT\_OF\_EEPROM\_ERROR Insufficient NV-Memory to complete command
- 0x1C = ILLEGAL\_COMMAND\_CODE Command code not supported
- 0x1E = INTEGRITY\_ERROR CRC or MAC does not match data Padding bytes not valid
- 0x40 = NO\_SUCH\_KEY Invalid key number specified
- 0x7E = LENGTH\_ERROR Length of command string invalid

- 0x9D = PERMISSION\_DENIED Current configuration / status does not allow the requested command
- 0x9E = PARAMETER\_ERROR Value of the parameter(s) invalid
- 0xA0 = APPLICATION\_NOT\_FOUND Requested AID not present on PICC
- 0xA1 = APPL\_INTEGRITY\_ERROR Unrecoverable error within application, application will be disabled
- 0xAE = AUTHENTICATION\_ERROR Current authentication status does not allow the requested command
- 0xAF = ADDITIONAL\_FRAME Additional data frame is expected to be sent
- 0xBE = BOUNDARY\_ERROR Attempt to read/write data from/to beyond the file's/record's limits. Attempt to exceed the limits of a value file.
- 0xC1 = PICC\_INTEGRITY\_ERROR Unrecoverable error within PICC, PICC will be disabled
- 0xCA = COMMAND\_ABORTED Previous Command was not fully completed Not all Frames were requested or provided by the PCD
- 0xCD = PICC\_DISABLED\_ERROR PICC was disabled by an unrecoverable error
- 0xCE = COUNT\_ERROR Number of Applications limited to 28, no additional CreateApplication possible
- 0xDE = DUPLICATE\_ERROR Creation of file/application failed because file/application with same number already exists
- 0xEE = EEPROM\_ERROR Could not complete NV-write operation due to loss of power, internal backup/rollback mechanism activated
- 0xF0 = FILE\_NOT\_FOUND Specified file number does not exist
- 0xF1 = FILE\_INTEGRITY\_ERROR Unrecoverable error within file, file will be disabled

## Files

Not shure yet what these constants do.

crypto operations

- TDES = 00
- TKTDES = 40
- AES = 80

File types

- STANDARD\_DATA\_FILE = 00
- BACKUP\_DATA\_FILE = 01
- VALUE\_FILE = 02
- LINEAR\_RECORD\_FILE = 03

- CYCLIC\_RECORD\_FILE = 04

#### Transmission modes

- PLAIN\_COMMUNICATION = 00
- PLAIN\_COMMUNICATION\_MAC = 01
- FULLY\_ENCRYPTED = 02

# Getestet Reader und Treiber

ACS ACR122U-A9 | Microsoft Usbccid-Smartcard-Leser (WUDF) | Windows 10

---

Version #1

Erstellt: 15 Oktober 2024 10:52:25 von Mario Voigt (Stadtfabrikanten e.V.)

Zuletzt aktualisiert: 25 Februar 2025 21:22:13 von Mario Voigt (Stadtfabrikanten e.V.)