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
- Mifaire DESFire Application
- DESFire Authentification
- DESFire Light Authentification 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 00 39 08

Instructions DESFire (used inside ADPU)

CLA = 0x90 APDU Sturuktur -> 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_DELIGATE_APPLICATION (EV2 only)
- 0xDA = DELETE_APPLICATION
- 0x6A = GET_APPLICATION_IDS
- 0x6E = FREE_MEMORY
- 0x6D = GET_DF_NAMES
- 0x?? = GET_DELIGATE_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: 2024-10-15 10:52:25 CEST von Mario Voigt (Stadtfabrikanten e.V.)
Zuletzt aktualisiert: 2025-02-25 21:22:13 CET von Mario Voigt (Stadtfabrikanten e.V.)