uFR Desfire Example - Simple

iOS

v1.3

Digital Logic Ltd.

Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

Table of contents

Digital Logic Ltd.

Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

About

Software example written in Swift programming language showcasing basic read/write operations with Desfire® cards.
This software currently supports uFR Online Series readers only.

Git repository: https://www.d-logic.com/code/nfc-rfid-reader-sdk/ufr-ds-examples-ios

uFR Series NFC Reader API: https://www.d-logic.com/code/nfc-rfid-reader-sdk/ufr-doc.git

Digital Logic Ltd.

Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

Usage

Communication with the reader

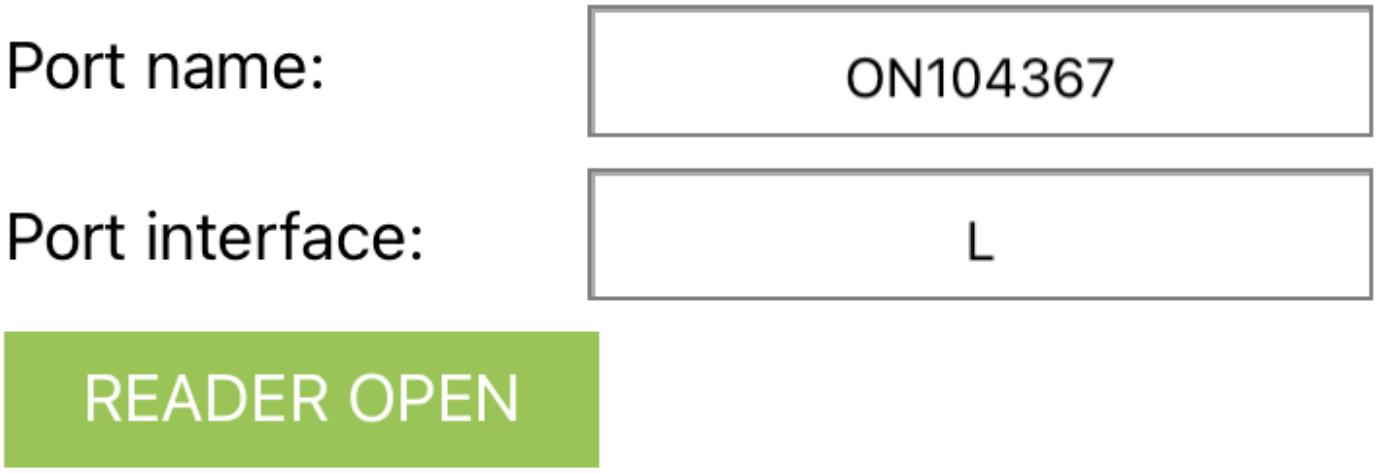
By providing "Port name" and "Port interface" parameters, users can specify desired communication type to be established with the reader via the **READER OPEN** button.

BLE

To start the communication via BLE, parameters should be in the following format:

- Port name: ONXXXXXX_BLE or simply ONXXXXXX. This parameter should contain the reader serial number with "ON" as the prefix, followed by the serial number and optional "_BLE" suffix.
- Port interface: 'L' or 76 (decimal).

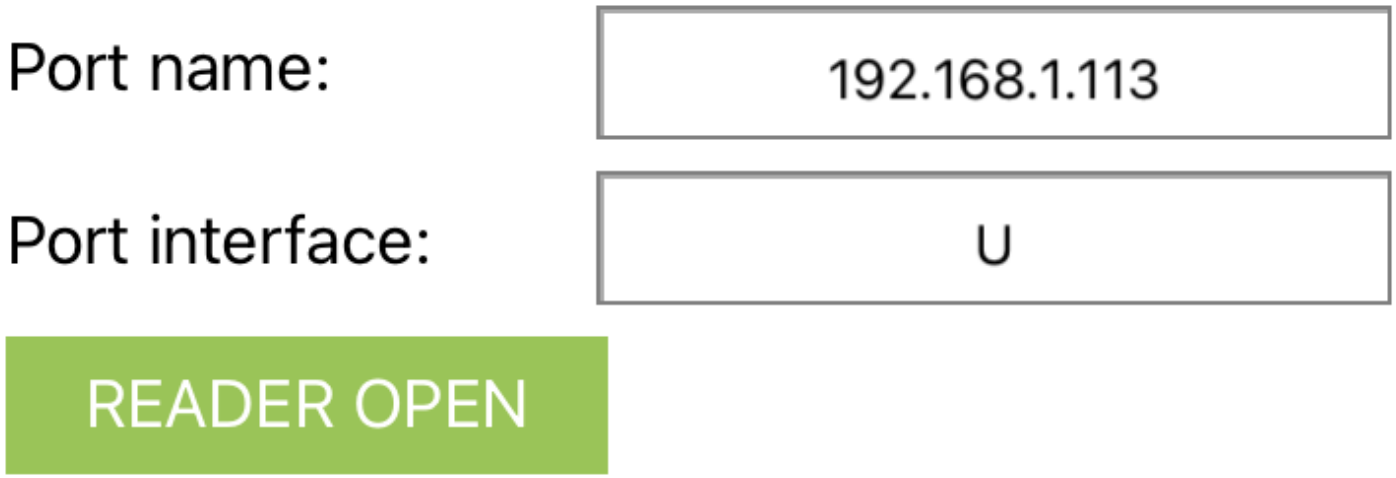
For example, as shown below:



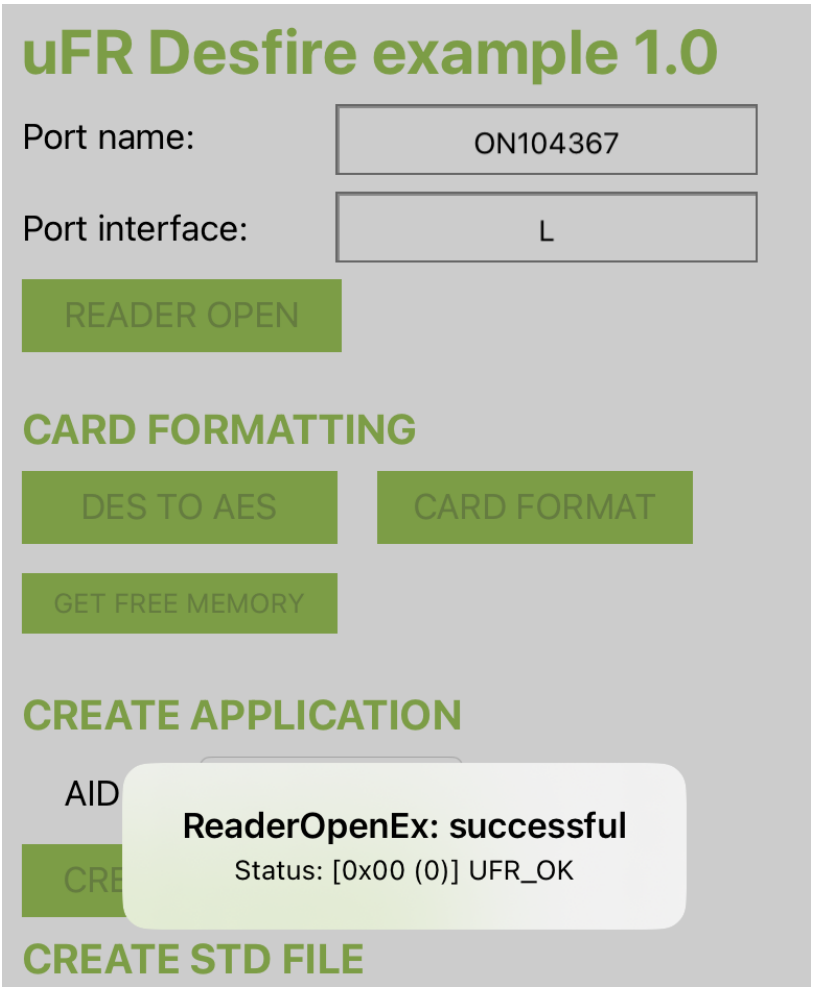
UDP/TCP

To start the communication via UDP/TCP, parameters should be in the following format:

- Port name: should contain the IP address of the reader on the same network.
- Port interface: 'U' or 85 (decimal) for UDP, 'T' or 84 for TCP.



Using the **READER OPEN** button, based on the parameters provided, the software will try to connect to the reader and display a status message informing you of the results:



Digital Logic Ltd.
Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

Card formatting

This software includes the following:

- Switching card master key from DES to AES
- Formatting card via AES master key
- Getting available free memory

DES to AES

By using the provided **DES TO AES** button, the user will switch the card master key from the default DES key to the AES key.
This option relies on using default DES key (8 0x00 hex bytes) to authorize key change to AES (new key will be 16 0x00 hex bytes)

Card format

Card format serves to wipe the tag clean and reset back to defaults. All the created applications and files on the card will be erased.
This method relies on the card's **master** key for formatting and will use the AES reader key stored in index 0 for authentication.

Digital Logic Ltd.
Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

Get free memory

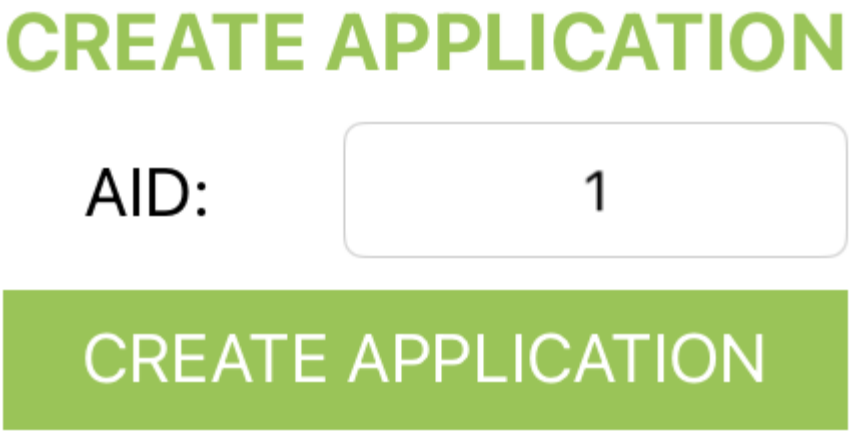
Simply serves the purpose of getting information about free memory left on the tag.
No authentication is necessary.

Authentication

This software will use **AES** keys and the reader key stored on index **0** for authentication.
Any changes to this reader key will affect future card operations.

Creating the applications and files

Create application



By providing a valid AID (Application Identifier) in the designated text field and using the **CREATE APPLICATION** button, a new Desfire® application will be created on the tag.
Valid AIDs for creation by default are in the range from 0x000001 to 0xFFFFFF
Application ID 0 (0x000000) is usually already defined and contains the card's master key.
Newly created application will have a maximum number of keys set to **1** and application setting set to **15 (0x0F)** - which implies the following:

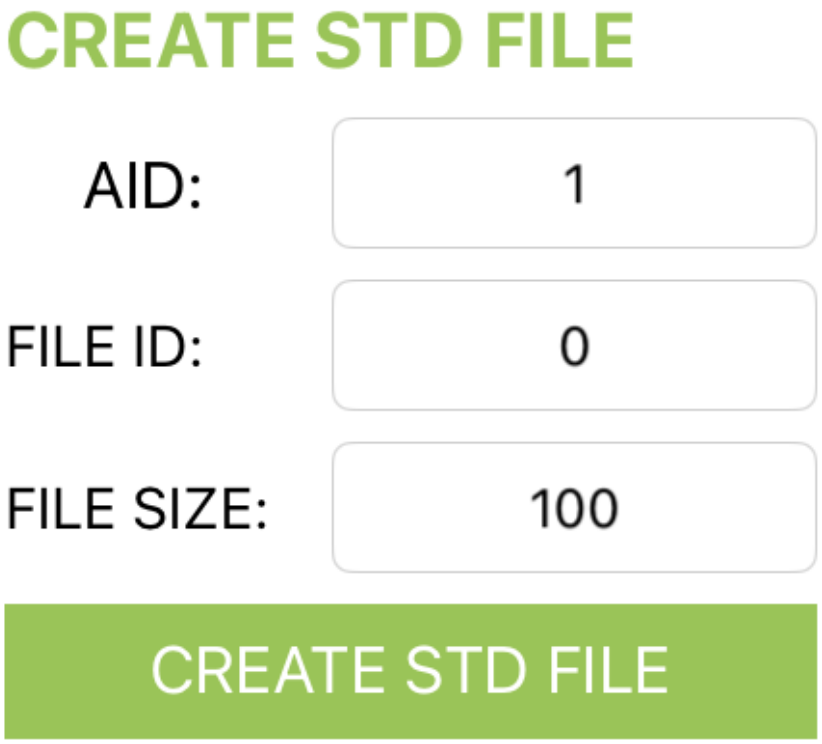
- Application settings are changeable
- Create/Delete file(s) without master key authentication
- Directory list without authentication

Digital Logic Ltd.
Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

- Application Master key is changeable

Details about these predetermined parameters when creating an application, and more, can be found in our **uFR Series NFC Reader API**: https://www.d-logic.com/code/nfc-rfid-reader-sdk/ufr-doc.git
Method used for application creation in this software is: **uFR_int_DesfireCreateAesApplication_aes**

Create Std data file



By using the **CREATE STD FILE** button, based on the AID, new FILE ID and FILE SIZE, a file that will be used for reading/writing operations will be created on the tag.
Valid FILE IDs for creation are in the range of 0-31. Every AID can have up to 32 files and the number of AIDs can be expanded based on the card's size.
File creation is set to be authenticated via reader key 0 and communication settings are set to 0 - PLAIN.
Newly created file will have its keys for reading, writing, read/write and change set to application key 0.

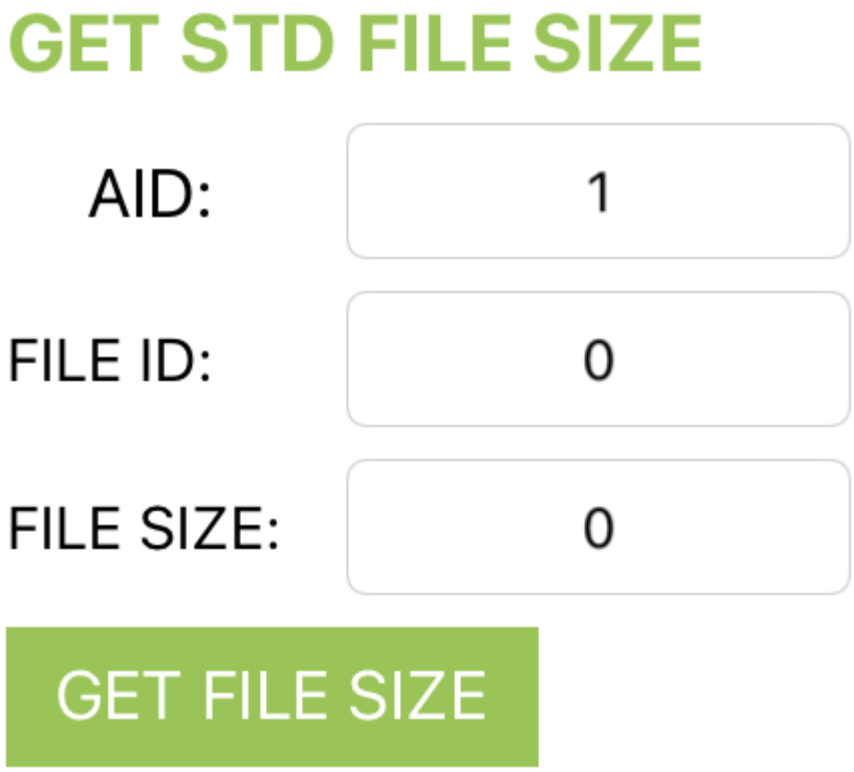
Details about these predetermined parameters when creating a Std data file, and more, can be found in our **uFR Series NFC Reader API**: https://www.d-logic.com/code/nfc-rfid-reader-sdk/ufr-doc.git
Method used for application creation in this software is: **uFR_int_DesfireCreateAesApplication_aes**

Important: File size **cannot** be changed after the file is created. Upon file deletion from the card, a memory that was allocated based on the file size provided **will not be freed** until the card is formatted via **FORMAT CARD** button. Upon file deletion, file id is available and file can be created again with the same file id.

Digital Logic Ltd.

Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

Get file size



By using the **GET FILE SIZE** button, the user can retrieve information about the size of the existing std data file on the card.
Valid **AID** and **FILE ID** are mandatory for this operation.
Parameters returned on success are:

- **File size:** total amount of data that this file can store.

Read/Write to file

Reading the file

By specifying the AID in which the file is stored, the FILE ID of the file and the LENGTH of the data and using the **READ FILE** button, the reader will try to read and display the data in the selected format.

Digital Logic Ltd.
Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

DATA: HEX ASCII

00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00

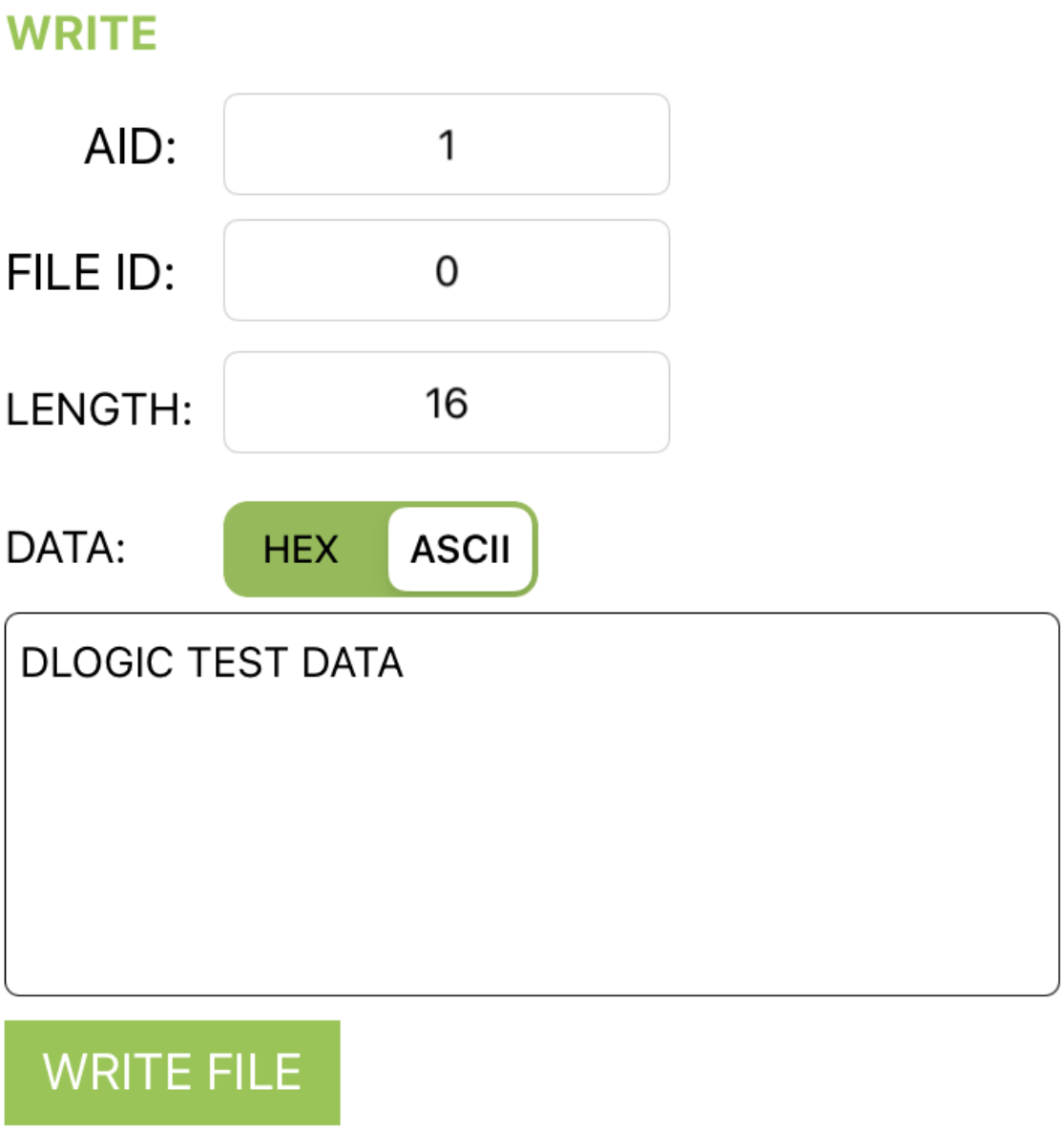
READ FILE

Digital Logic Ltd.
Address: Nemanjina 57a, 12000 Pozarevac, Serbia · **Tel:** +38112541022· **VAT:** 111385444 **Reg.** 21473642
e-mail: office@d-logic.com · www.d-logic.com

Writing to the file

Same parameter format applies as with the previous READ option.
Provide the AID and FILE ID of the file, and finally input the data. The LENGTH field will be populated as the user enters the data and will display the length of the current input.

Finally, use the **WRITE FILE** button to store the data on the tag, in the selected format.



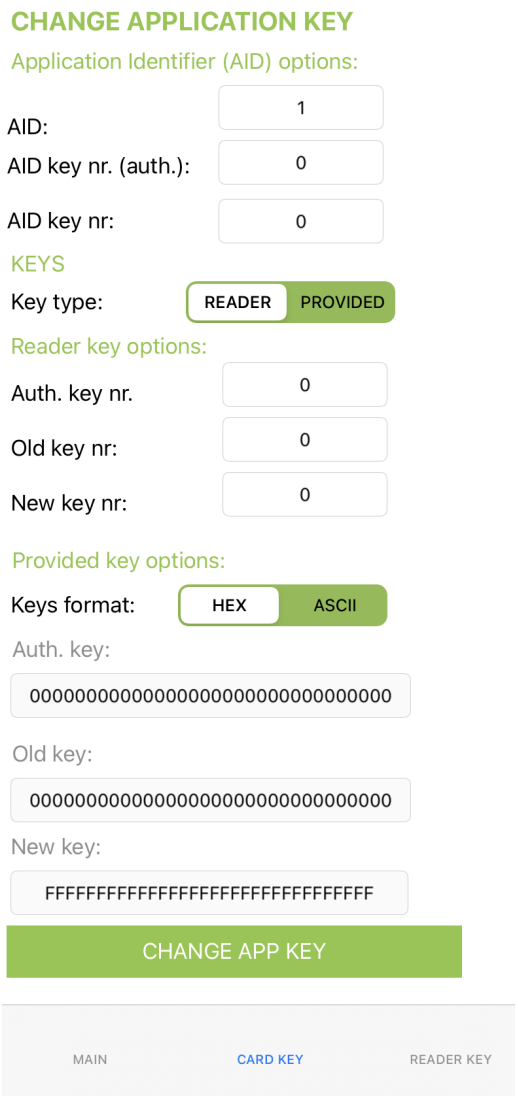
Digital Logic Ltd.
Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

Method used for reading/writing data in this software are:

- **uFR_int_DesfireReadStdDataFile_aes**
- **uFR_int_DesfireWriteStdDataFile_aes**

Details about the methods used for reading/writing data can be found in our **uFR Series NFC Reader API**: https://www.d-logic.com/code/nfc-rfid-reader-sdk/ufr-doc.git

Card key write



These options give access to changing keys stored on the Desfire® card based on the parameters provided and card key settings.

Digital Logic Ltd.
Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

When changing the key for **AID 0** - you will be notified that it will be the **card master key** that will be changed, in this case, parameters **AID key nr. (auth.)** and **AID key nr.** will be ignored since they are related to the other card applications that contain more than one key and have their AID different from 0.

Parameters

Application identifier options (AID):
AID - Application Identifier whose key will be changed
AID key nr (auth.) - Index of the application key that will be used to authenticate key changing.
AID key nr. - Index of the application key that will be changed

Key type: Specifies the input source of the keys. Whether using the keys stored in the uFR reader or providing them manually in the designated fields below (Under **Provided key options**)

Reader key options:
Auth. key nr - Reader key index that will be used for the authentication
Old key nr - Key that will be changed, provided from the reader.
New key nr - New key to be stored in the card, provided from the reader.

Provided key options:
Keys format - Specifies format of the provided keys. **HEX** input requires 16 hex bytes, **ASCII** requires 16 characters long keys.

Auth key - Provided key that will be used to authenticate card key change operation
Old key - Provided old key that currently exists on the card
New key - Provided new key that will be stored on the card.

Methods used for changing keys in this example are:

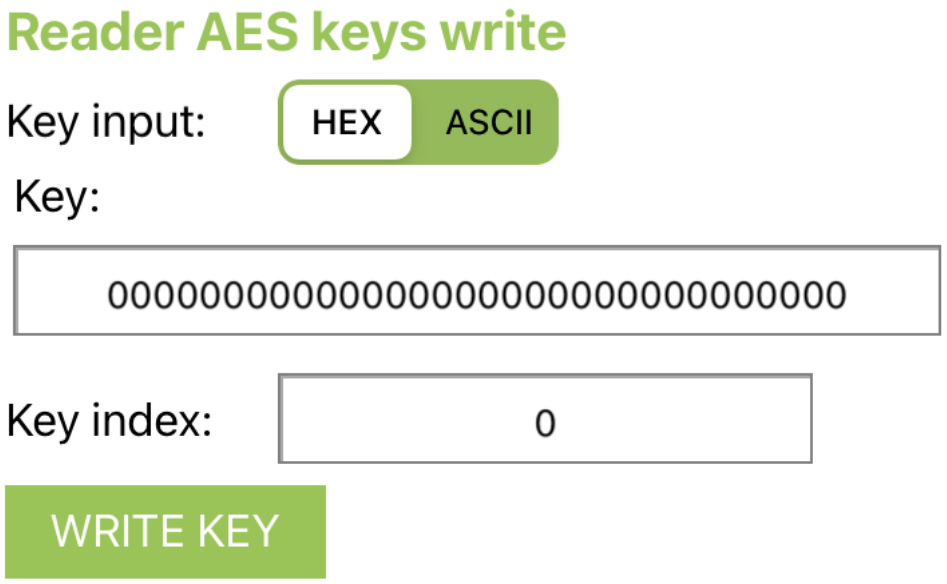
- **uFR_int_DesfireChangeMasterKey**(_PK) - when changes are made to the card Master key, and
- **uFR_int_DesfireChangeAesKey_aes**(_PK) - when changing card application keys

For more details on how these methods work, refer to **uFR Series NFC Reader API**:
https://www.d-logic.com/code/nfc-rfid-reader-sdk/ufr-doc.git

Digital Logic Ltd.
Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

Reader key write

Switch to the tab **READER KEY** in the lower right corner of the software to gain access to these options.



By using the **WRITE KEY** button, the AES key will be stored in the reader based on the KEY INDEX provided. The available key index range for AES keys is 0-15.

Digital Logic Ltd.

Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

Revision history

Date	Version	Comment
2023-03-23	1.3	Get file size section added.
2023-02-01	1.2	DES to AES updated.
2023-01-31	1.1	Card key write section added. Create application, Create Std data file sections updated. Document renamed.
2023-01-27	1.0	Base document

Digital Logic Ltd.

Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com