uFR Desfire Example - Advanced

iOS

v1.1

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 card read/write and card key change 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

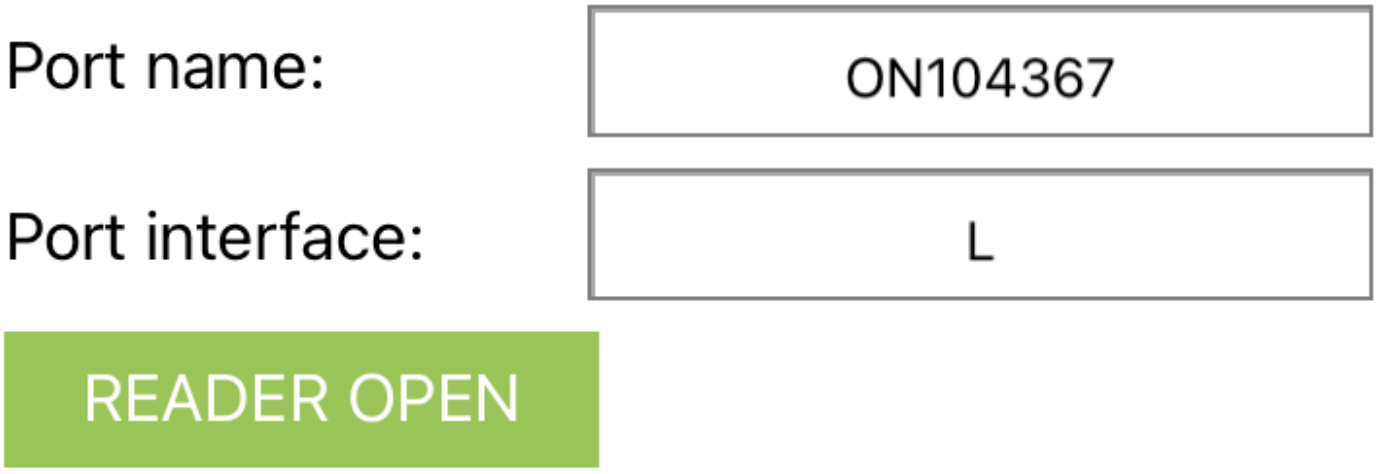
By providing "Port name" and "Port interface" parameters, users can specify desired communication type to be established with the reader via the **READER OPEN** button.

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).

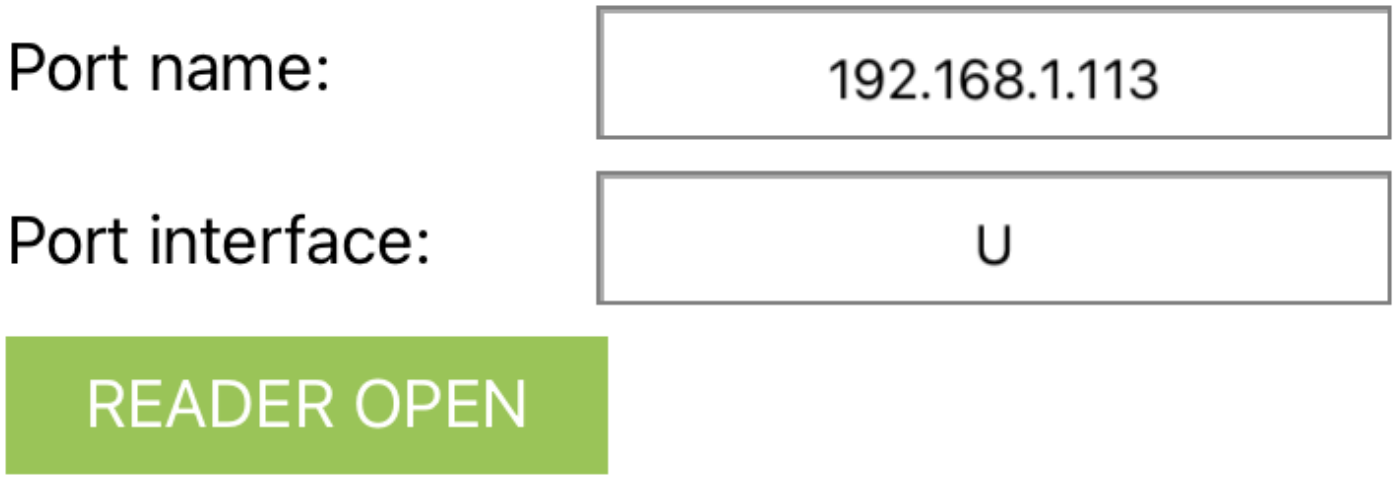
For example, as shown below:



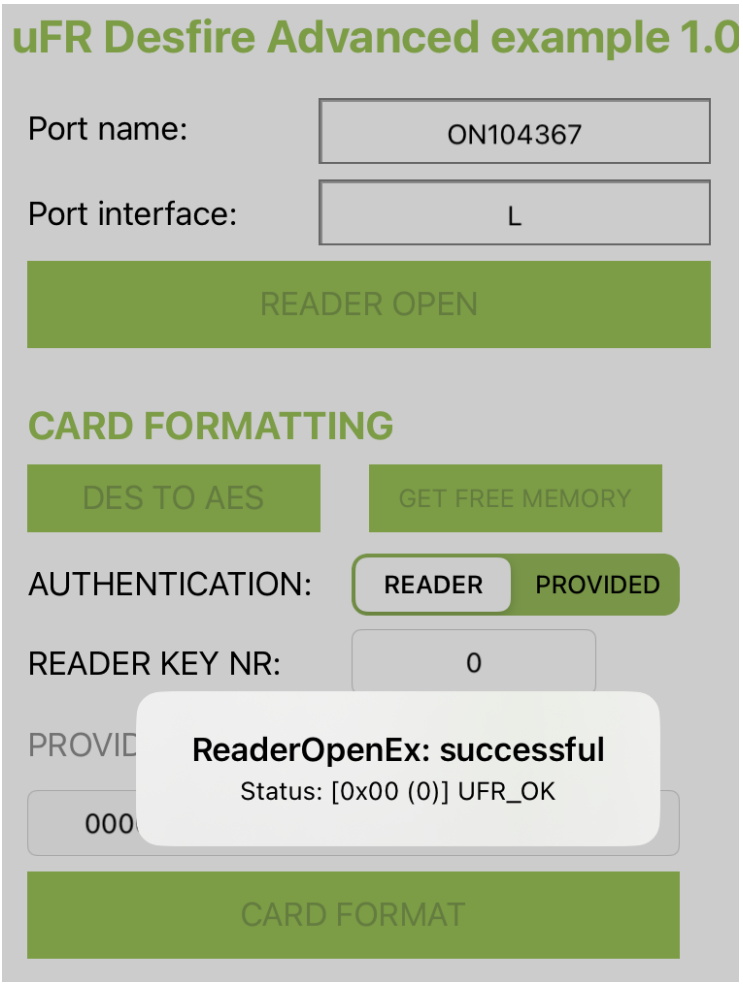
UDP/TCP

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:

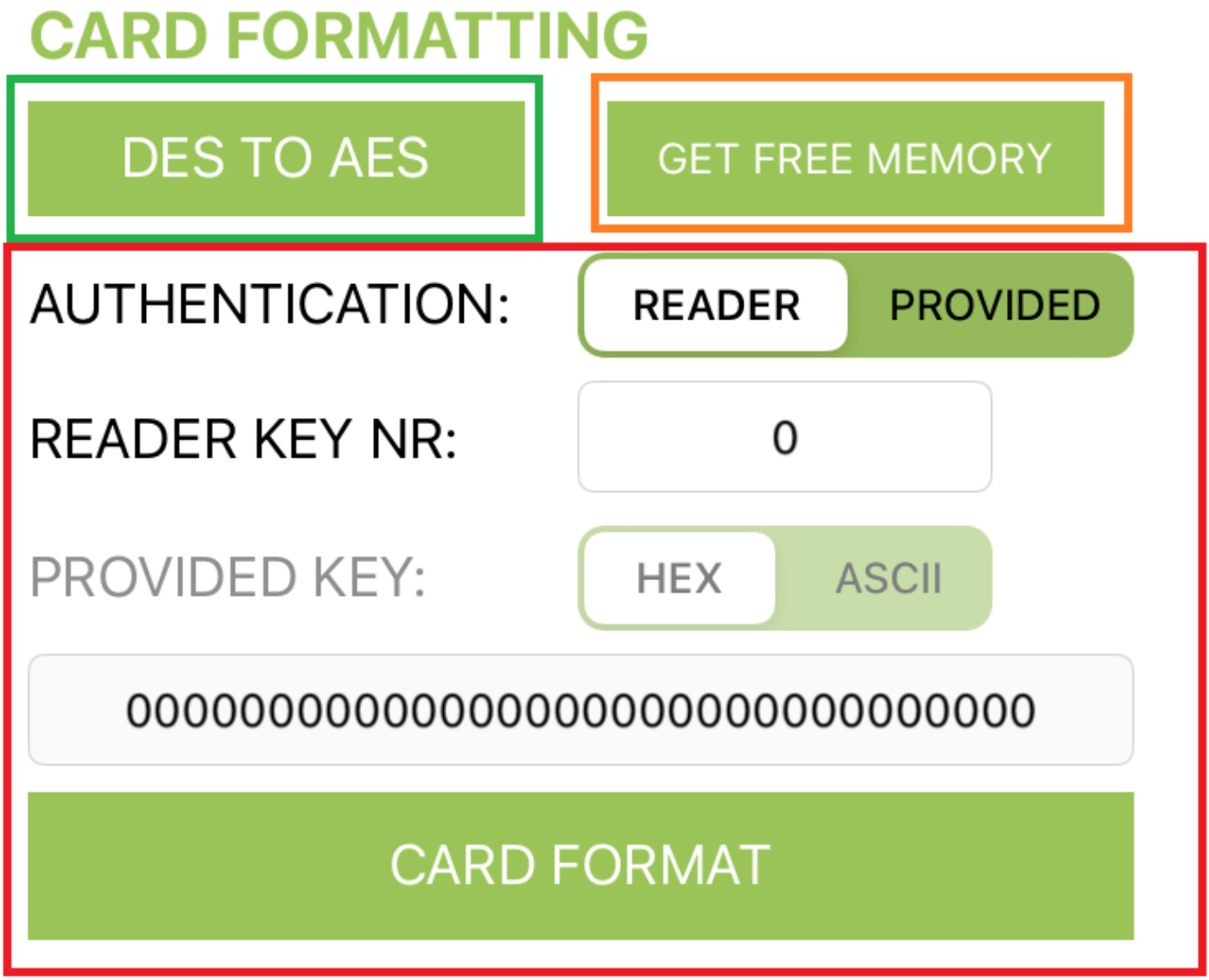


Digital Logic Ltd.
Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

Card formatting

This software includes the following:

- Switching card master key from DES to AES
- Getting available free memory
- Formatting card via AES master key from the reader or providing one in the designated field



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

DES to AES

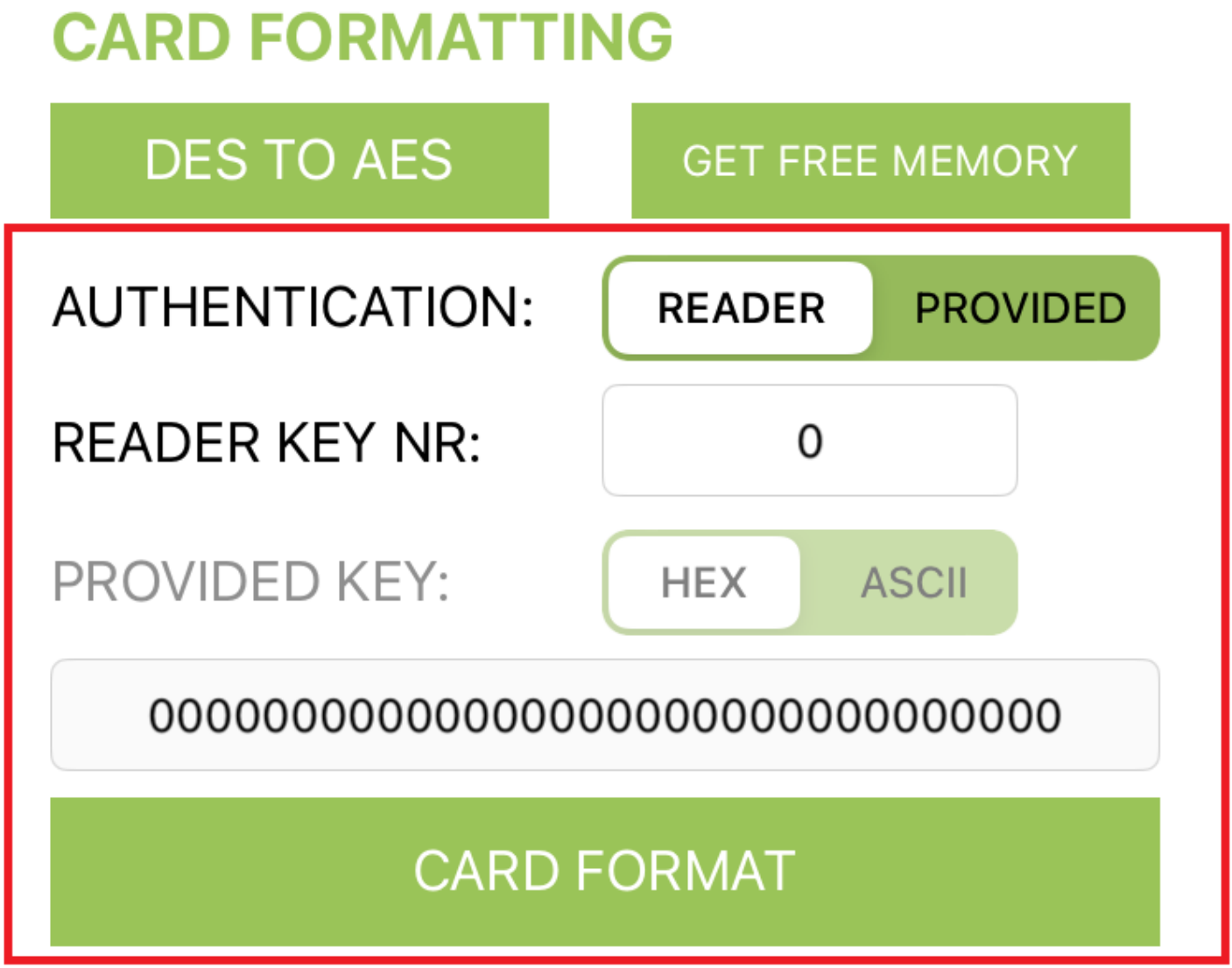
By using the provided **DES TO AES** button, the user will switch the card master key from the default DES key to the AES key.
This option relies on using default DES key (8 0x00 hex bytes) to authorize key change to AES (new key will be 16 0x00 hex bytes)

Get free memory

Button **GET FREE MEMORY** simply serves the purpose of getting information about free memory left on the tag.
No authentication is necessary.

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 format



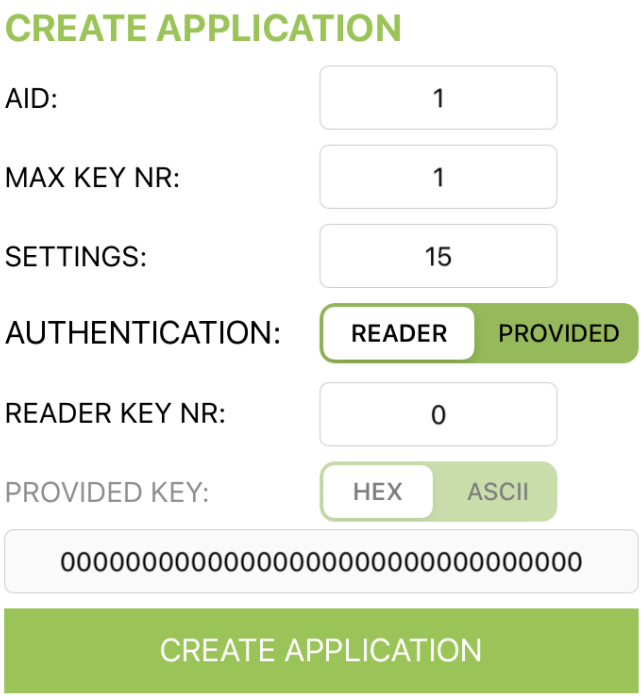
Card format serves to wipe the tag clean and reset back to defaults. All the created applications and files on the card will be erased.
This method relies on the card's **master** key for formatting.

Highlighted options above are used for this action.
Depending on the users' **AUTHENTICATION** selection, it will be necessary to provide either a valid key index stored in the reader (**READER KEY NR**) or manually input AES key in the **PROVIDED KEY** field.

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

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.

Other parameters necessary for creating an application are:

- **MAX KEY NR**: Defines maximum number of keys in the newly created application. Application can have up to 14 keys stored.

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

- **SETTINGS**: Defines application master key settings. Valid values are in range 0-15 and the values are calculated in the following manner

Bit 3	Bit 2	Bit 1	Bit 0
If set to 1 - Allows a future change of this configuration	If set to 1 - Master key is not required for creation/deletion of card applications	If set to 1 - allows directory list access without master key authentication	If set to 1 - allows master key change

By default, **master key settings** have value of **15** (binary: **00001111**)

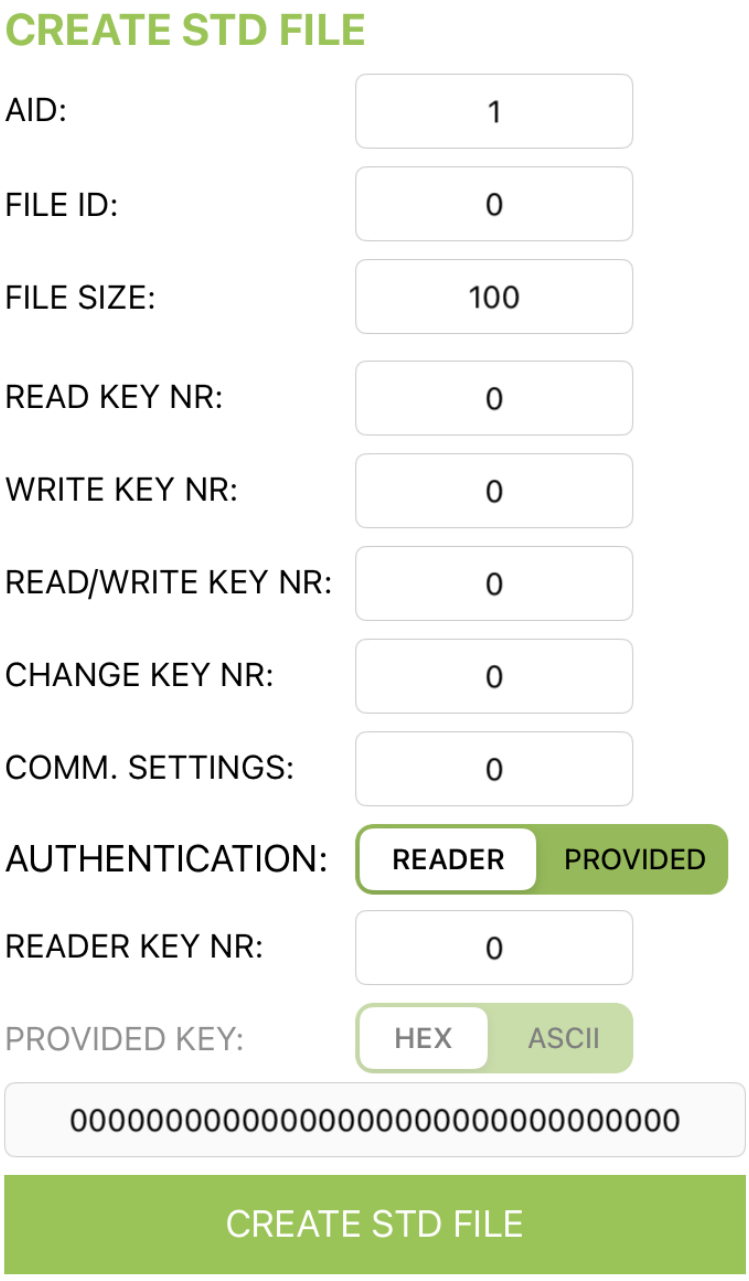
- **AUTHENTICATION**: Depending on the users selection, card operation will be authorized using the key stored in the reader, or the one provided manually in the designated **PROVIDED KEY** field.

Details about these 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 are:

- **uFR_int_DesfireCreateAesApplication_aes**
- **uFR_int_DesfireCreateAesApplication_aes_PK**

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

Create Std data file



By using the **CREATE STD FILE**, a file that will be used for reading/writing operations will be created on the tag based on the parameters provided.

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

Valid **FILE ID**s for creation are in the range of 0-31. Every AID can have up to 32 files and the number of **AID**s can be expanded based on the card's size.

Other parameters used for creation:

- **FILE SIZE**

Used to determine the size of the new file in bytes.

- **READ KEY NR**
- **WRITE KEY NR**
- **READ/WRITE KEY NR**
- **CHANGE KEY NR**

Used to determine card access rights. Values in range **0-13** will reference the application key with this number to authorize the related card operation.
If a value is set to **14** "free access" is granted, implying that card operation will require no previous authorization.
However, if set to **15**, "deny access" is set. For example, if **WRITE KEY NR** is set, file type will be set to **READ ONLY**.

- **COMM. SETTINGS**

Communication settings. Plain communication settings value is 0x00; Communication secured by MACing, value is 0x01; Fully enciphered communication setting, value is 0x03

Authentication of this operation can be done via reader key or manually with the provided key.

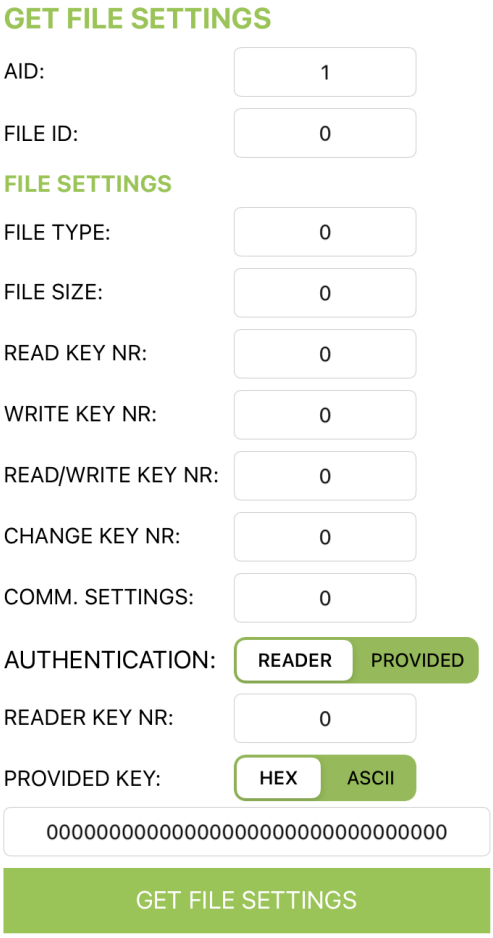
Important: File size **cannot** be changed after the file is created. Upon file deletion from the card, a memory that was allocated based on the file size provided **will not be freed** until the card is formatted via **FORMAT CARD** button. Upon file deletionfile can be created again with the same file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

Details about these 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 are:

- **uFR_int_DesfireCreateAesApplication_aes**
- **uFR_int_DesfireCreateAesApplication_aes_PK**

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

Get file settings



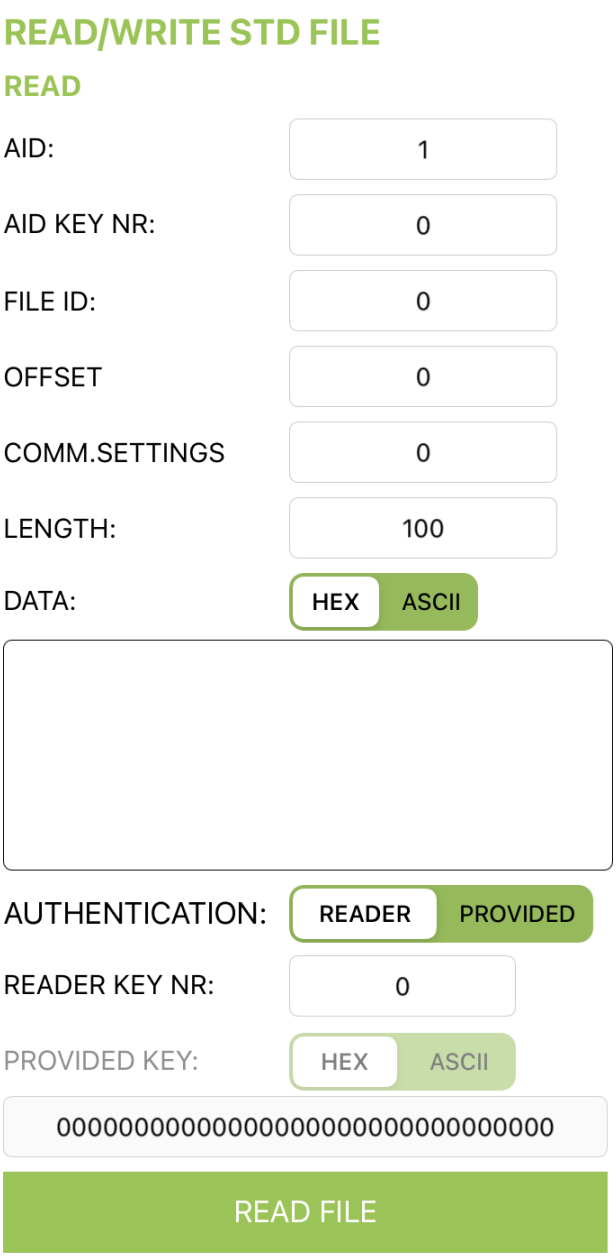
By using the **GET FILE SETTINGS** button, the user can retrieve information about the created std data file. Valid **AID** and **FILE ID** are mandatory for this operation.
Parameters returned on success are:
File type - 0 indicates it is STD data file
File size - total amount of data that this file can store
Read key nr - read access settings for this file (configured while creating the filet)
Writekey nr - write access settings for this file (configured while creating the file)
Read/Write key nr - read/write access settings for this file (configured while creating the file)
Change key nr - Change settings access for this file (configured while creating the file)
Comm. settings - communication mode set for this file (configured while creating the file)

Authentication of this operation can be done via reader key or manually with the provided key.

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

Read/Write to file

Reading the file



By specifying the necessary parameters 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

Parameters for card read operation are:

- **AID**

Application identifier that contains the file

- **AID KEY NR**

Application key that will be referenced when reading the data for the purpose of authorization.

- **FILE ID**

ID of the file that will be read

- **OFFSET**

Starting position when reading, offset **0** will start reading from the beginning of the file.

- **COMM. SETTINGS**

As mentioned previously, can be 0 - PLAIN, 1-MACked, 3-ENCIPHERED

- **LENGTH**

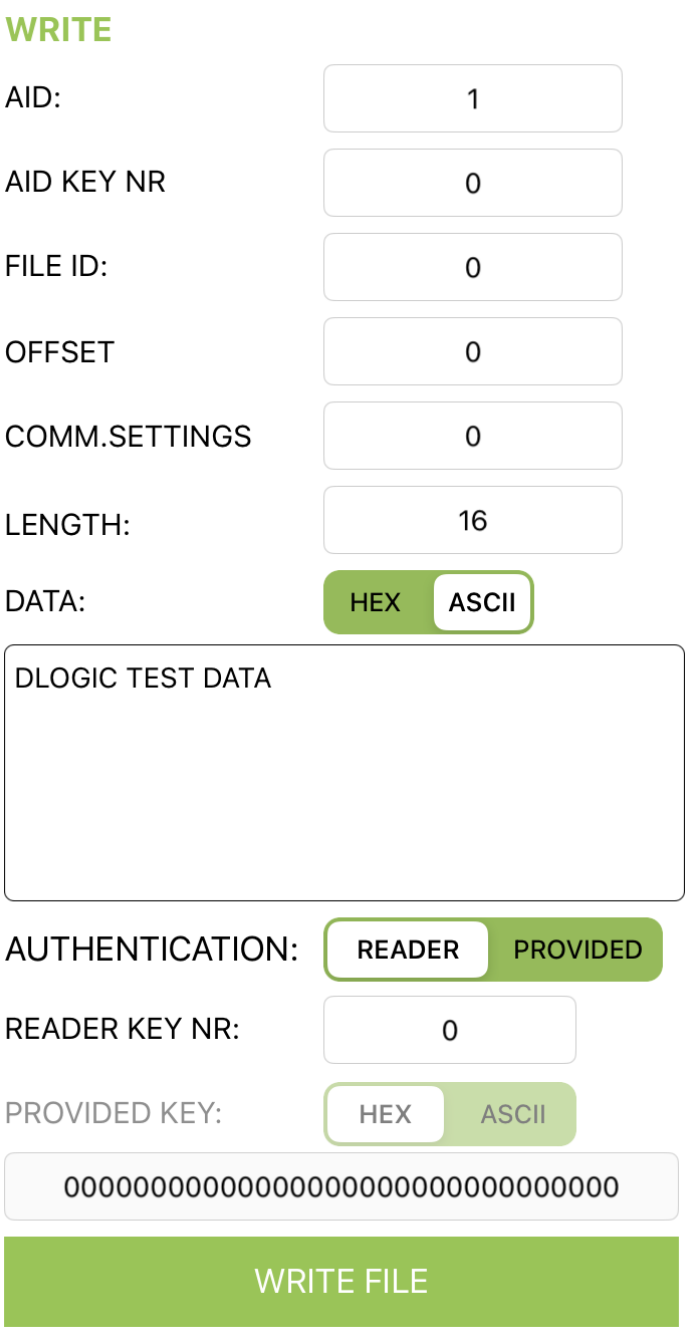
Amount of data to be read expressed as number of bytes.

- **DATA**

Successfully read data will be displayed in this field, based on the selected **HEX** or **ASCII** format

Authentication of this operation can be done via reader key or manually with the provided key.

Writing to the file



Same parameter format applies as with the previous **READ** option.

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

Provide the **AID** and **FILE** ID of the file, and finally input the data. The **LENGTH** field will be populated automatically as the user enters the data and will display the length of the current input. Length will be calculated based on the format selected (HEX/ASCII).

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

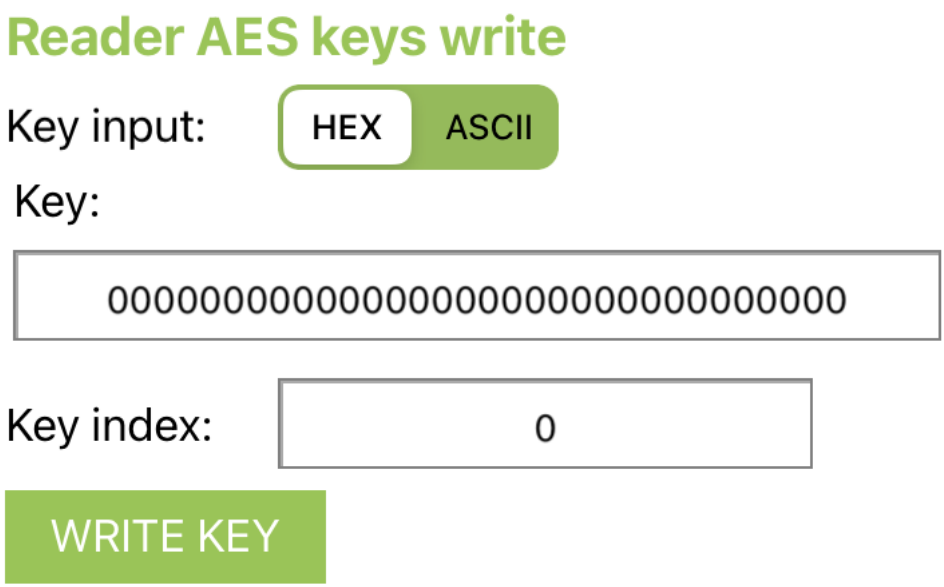
Method used for reading/writing data in this software are:

- **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

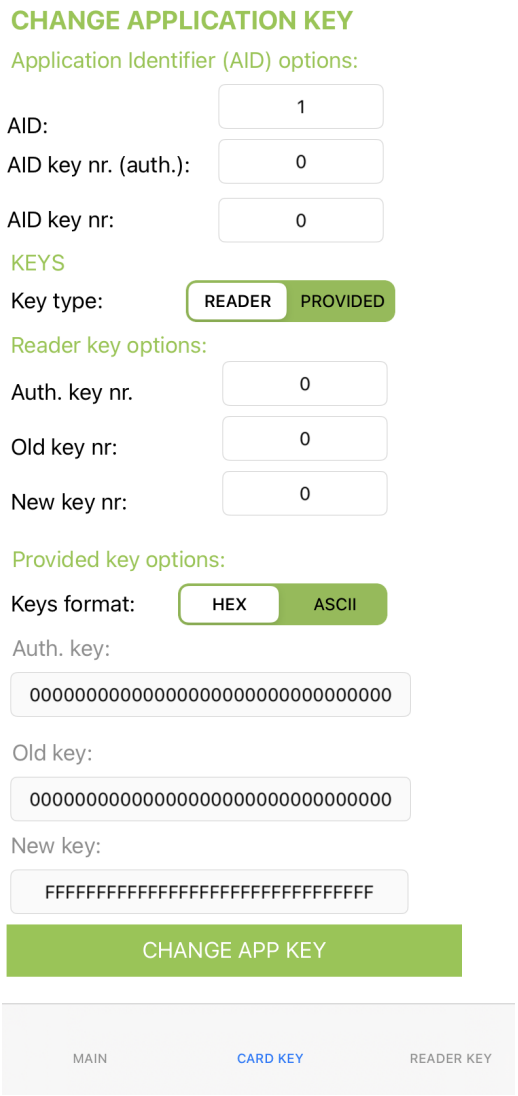
Reader key write

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.

Card key write



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

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

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

Revision history

Date	Version	Comment
2023-03-23	1.1	Get file settings section added.
2023-02-03	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