rf IDEAS

June 2020

User Guide to the Smartcard Manager, v1.5

Configuring readers for LEGIC®, MIFARE® DESFire® and MIFARE Classic®

Trust begins here.™

www.rfIDEAS.com

Table of Contents

1. Scope

This user guide describes how to use the Smartcard Manager application to configure rf IDEAS® readers. Readers that are capable of reading data fields from contactless cards require additional settings beyond our typical interfaces.

The Smartcard Manager will inform the reader what data bytes to read and what keys are needed to access that data. For keystroke readers, pcProxConfig can then be used as needed for additional formatting of keystroke output. For SDK access and MFP24 readers, Smartcard Manager is the only application needed.

Card types currently supported are LEGIC® (advant and prime), MIFARE Classic®, and MIFARE DESFire® (EV1/EV2/LEAF). Details of the cards are not included here, it is assumed that the reader is aware of the data structure (blocks, files or sectors) and what keys are needed for their particular card. There is a brief overview of how MIFARE keys are stored and the nomenclature as used by Smartcard Manager.

NOTE: All numeric entries in the GUI are in hexadecimal!

2. Standard Controls

Some controls can be accesssed at all times. The **Configure Reader** button at the bottom will send configuration data (not including keys) to the reader. Next to it is the status bar, where any error condition will be displayed in red.

There are several menu entries, some of which deserve special mention:

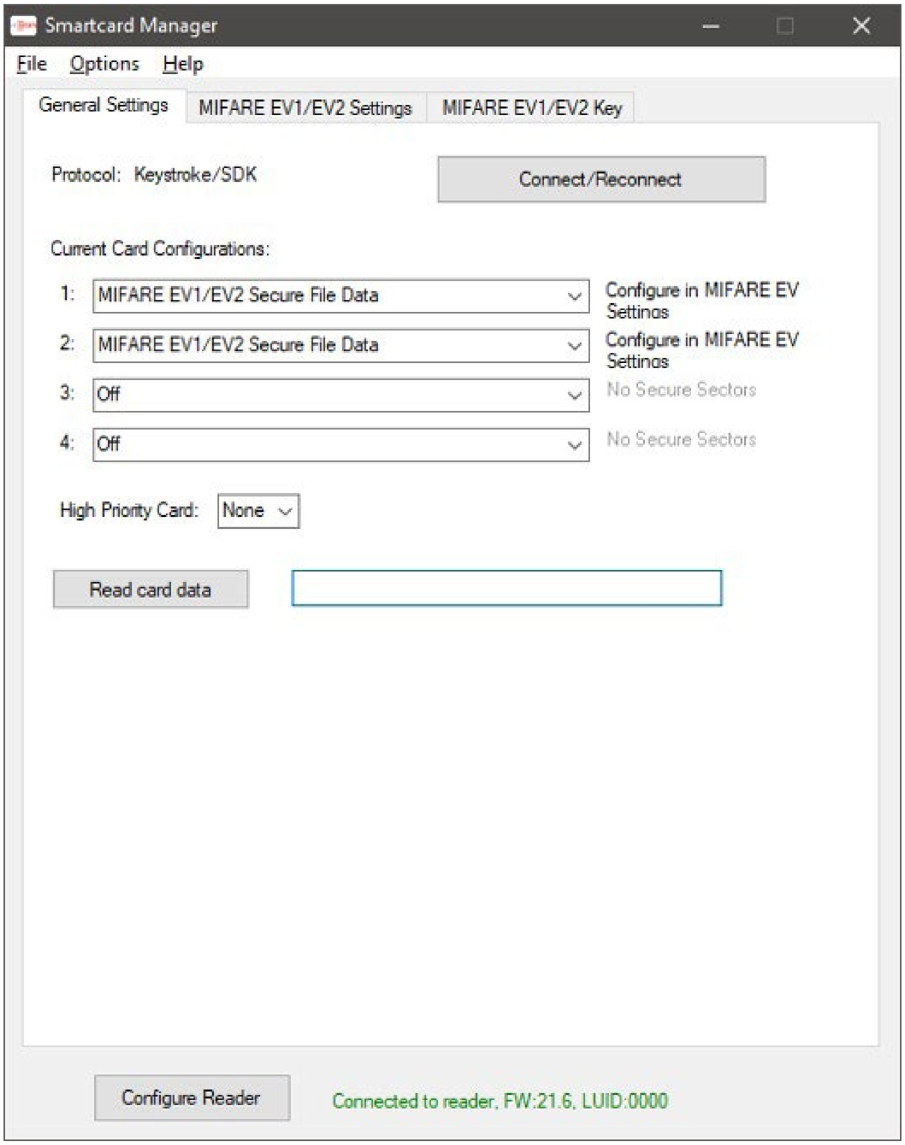
1. **File >** Save Configuration – save configuration settings, including keys, if entered, to the PC
2. **File >** Load Configuration – retrieve configuration settings from the PC
3. **File >** Start Trace Log File – captures actual USB messages to and from the reader
4. **Options >** Perform Beep Test – test the current connection by telling the reader to beep
5. **Help >** About Smartcard Manager, About Reader – display version and other information

The Save and Load Configuration options creates a readable .ini file for all settings and keys that are currently set in the active tabs. To avoid saving a key in a readable format, it is recommended to use the Encrypt button found in the key tab before saving the configuration.

3. General Settings

In the General Settings tab, **Connect/Reconnect** will establish a connection to the reader. This is useful when switching readers on the PC (it will only connect to one reader at a time). It reads the current configuration of the reader as part of the connection process.

The General Settings tab is used to configure card types, and additional tabs are used for specific MIFARE® or LEGIC® configuration and to send keys. The pcProxConfig utility can be used if additional settings are needed for specialized keystroke output, such as converting the data to decimal or ASCII output. There can be multiple secure file configurations set at one time, and a mix of MIFARE DESFire® EV1/EV2 and MIFARE Classic®. LEGIC readers do not read MIFARE secure data and vice versa.



Protocol: Keystroke/SDK

Current Card Configurations:

1: MIFARE EV1/EV2 Secure File Data — Configure in MIFARE EV Settings

2: MIFARE EV1/EV2 Secure File Data — Configure in MIFARE EV Settings

3: Off — No Secure Sectors

4: Off — No Secure Sectors

High Priority Card: None

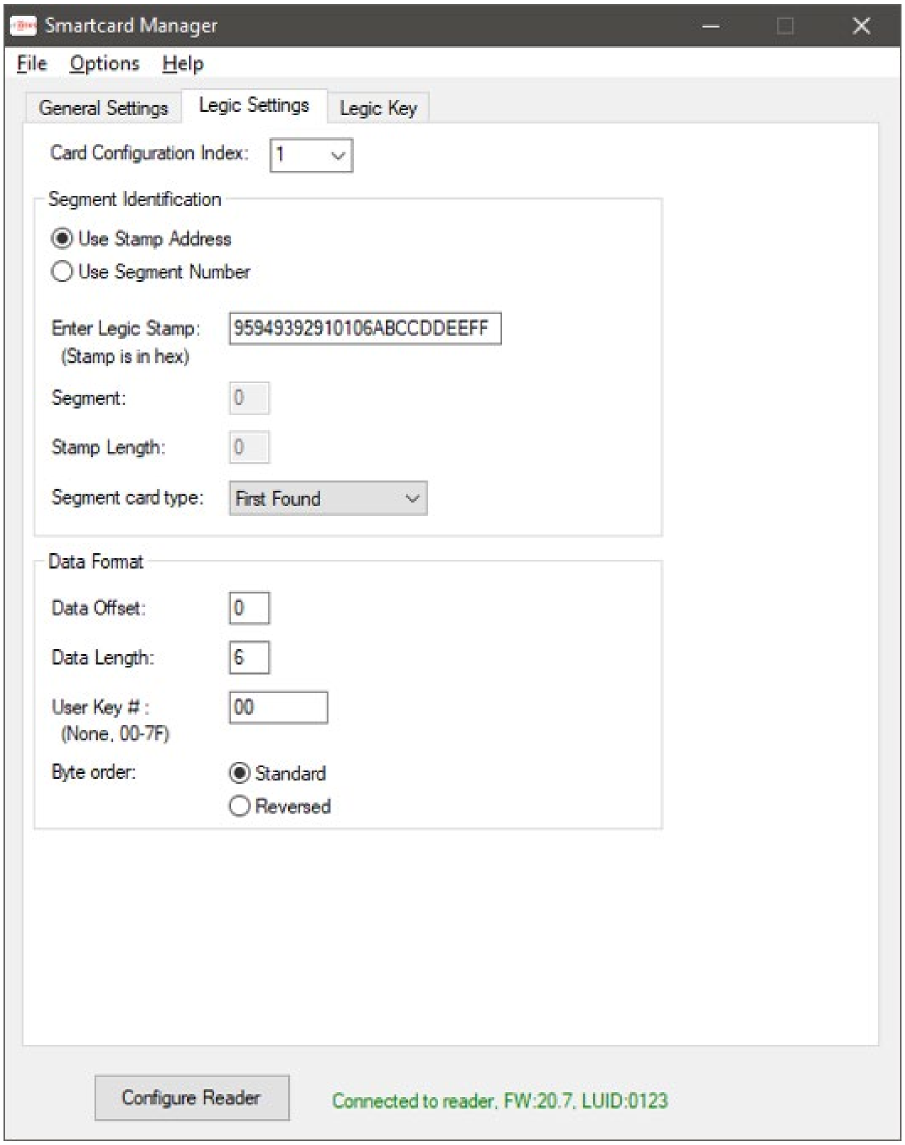
Connected to reader, FW:21.6, LUID:0000

If the same secure file data card type is selected for more than one configuration (as shown above), then the Card Configuration Index (1-4) in the subsequent tabs will determine which configuration is currently selected.

4. LEGIC® Settings and Key

If a card type is set to LEGIC Stamp, then a tab for LEGIC Settings will appear. For firmware version 20.7 and later, a tab for LEGIC Key will also appear.

The LEGIC settings tab has the following fields:



Card Configuration Index: 1

Segment Identification

● Use Stamp Address

○ Use Segment Number

Enter Legic Stamp: (Stamp is in hex) 95949392910106ABCCDDEEFF

Segment: 0

Stamp Length: 0

Segment card type: First Found

Data Format

Data Offset: 0

Data Length: 6

User Key # : (None, 00-7F) 00

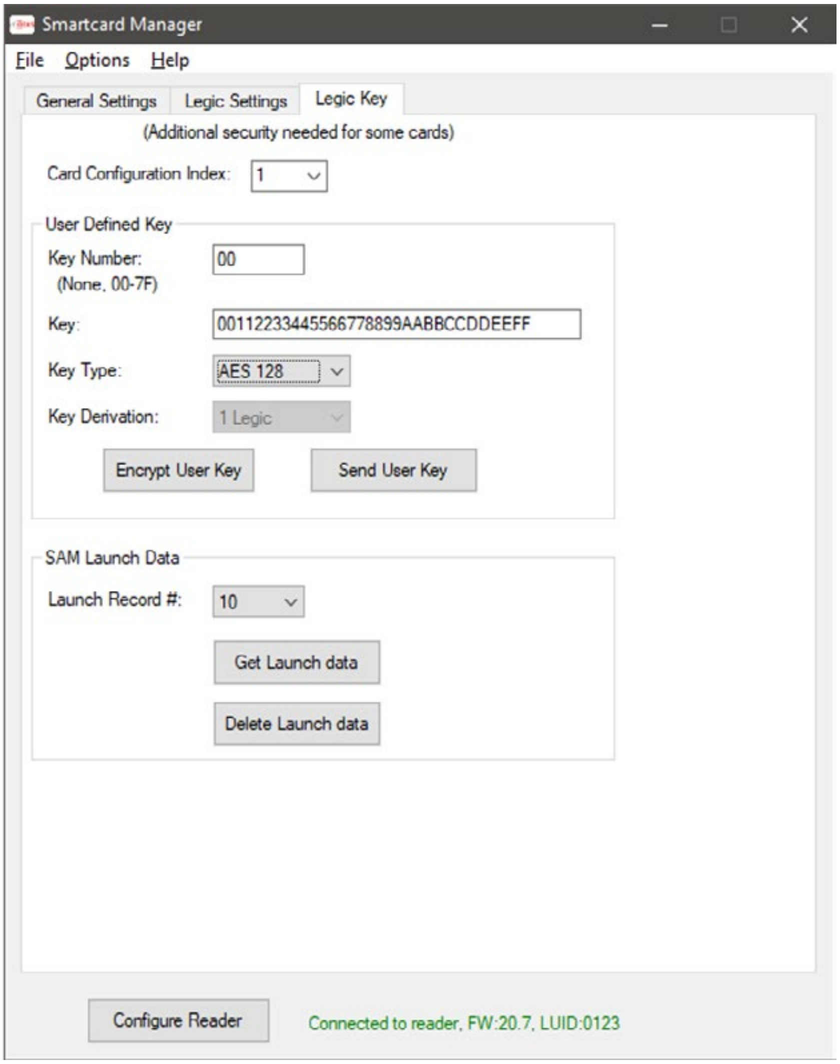
Byte order: ● Standard ○ Reversed

Connected to reader, FW:20.7, LUID:0123

A LEGIC segment can be addressed by the Stamp Address, or by the segment number. When using the segment number, an optional Stamp Length field is available. Entering this will keep the data consistent if both LEGIC advant and prime cards are being used, as the prime card includes the stamp with the card data, while the advant does not.

The Segment Card Type field is useful when using a multi-technology LEGIC® card. There are three LEGIC technologies: prime, advant on ISO-14443A, and advant on ISO-15693. On a multi-technology card, there will be a combination of technologies, each with its own range of segments, possibly using the same Stamp address. This field will determine which one is used, or "First Found" is non-discriminatory (default case, and best choice for the standard single-technology card).

For firmware versions 20.7 and later, a user-defined key number can be entered. This key number is an index to a table stored in the LEGIC chip. The actual key is entered in the next tab, the LEGIC Key tab.



(Additional security needed for some cards)

Card Configuration Index: 1

Key Number: 00
(None, 00-7F)

Key: 00112233445566778899AABBCCDDEEFF

Key Type: AES 128

Key Derivation: 1 Legic

Launch Record #: 10

Connected to reader, FW:20.7, LUID:0123

Note that the key is not sent to the reader when the Configure Reader button is pressed. There is a separate Send User Key button.

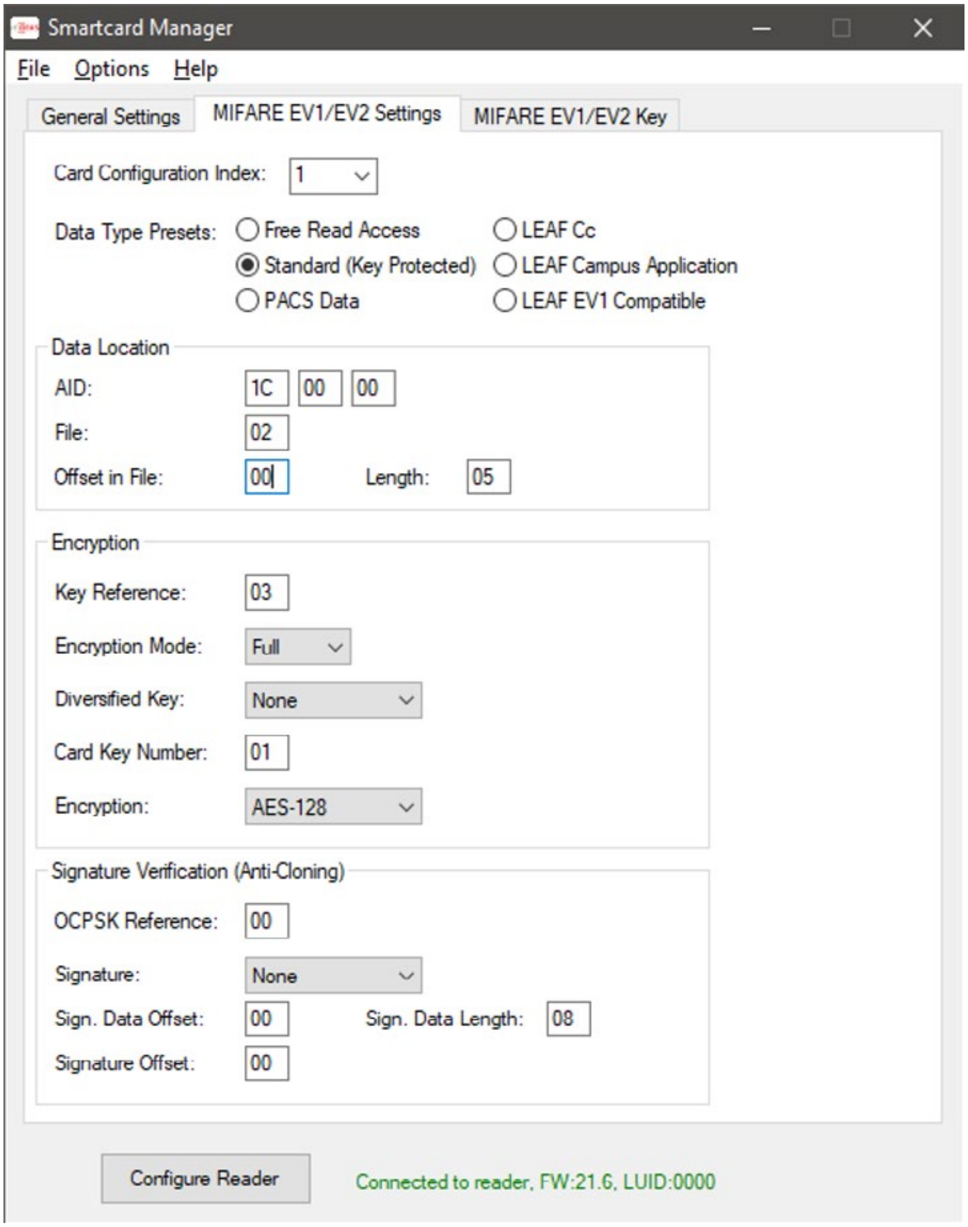
The key is entered on this tab, and stored at location Key Number in the LEGIC chip. The key cannot be read back. If desired, the key can be encrypted after it is entered. Thereafter it will be displayed in the encrypted form, stored in the configuration file as encrypted (if a configuration file is created), and it is sent encrypted over USB to the reader

The bottom section of this tab is used for Launch (baptism) using a SAM-63 card. Some user cards require that a reader be launched before the user data can be read. If LEGIC Stamp is selected as a card type, than any LEGIC reader (including 20.5) can be launched with a SAM-63 card.

In firmware 20.7 and later, when a SAM-63 card is detected in the field, the usual 15-second window for launching is reduced to 7 seconds, and a beep and/or LED change indicates the launch has occurred. This results in a record being stored in the LEGIC chip. This launch record can be read back, to verify it was launched, and it can also be deleted.

5. MIFARE® EV1/EV2 Settings

If a card type is set to MIFARE EV1/EV2 Secure File Data, then a tab for MIFARE EV1/EV2 Settings will appear. Selecting it will show the following fields needed for reading a DESFire® card:



Card Configuration Index: 1

Data Type Presets: ○ Free Read Access ○ LEAF Cc ● Standard (Key Protected) ○ LEAF Campus Application ○ PACS Data ○ LEAF EV1 Compatible

Data Location

AID: 1C 00 00

File: 02

Offset in File: 00 Length: 05

Encryption

Key Reference: 03

Encryption Mode: Full

Diversified Key: None

Card Key Number: 01

Encryption: AES-128

Signature Verification (Anti-Cloning)

OCPSK Reference: 00

Signature: None

Sign. Data Offset: 00 Sign. Data Length: 08

Signature Offset: 00

Connected to reader, FW:21.6, LUID:0000

The Data Type Presets at the top are a handy way to set the reader for common uses. For example, the LEAF Cc and LEAF EV1 Compatible presets will fill in the fields to read the Badge ID from a standard LEAF card. The other options are for more customizable data selection.

The rest of the page is organized into three blocks:

- **Data Location** – where the data is located on the card, and what bytes to return.
- **Encryption** – how the data is protected and with what key.
- **Signature Verification** – for optional anti-cloning protection.

Data Location:

The MIFARE® DESFire® cards store data in Application spaces, referred to by their Application ID (AID). Each AID has one or more Files where the data is stored. The AID is sometimes described in big endian format (most significant number first) or little endian format (least significan number first). Smartcard Manager uses the latter, following the lead of NXP tools, but card documentation may vary.

Encryption

The Key Reference is an index into keys stored on the SAM AV2 chip inserted into the reader. The Key can also be programmed at this time using the EV1/EV2 Key tab, or can be programmed at another time, even on a different reader or device. In any case, the Key Reference value on this page must match the Key ID used when storing the key. The index is a value in the range of hexadecimal values 01 to 7F.

A diversified key is modified, in part by the card's CSN, so the resulting key is unique to each card.
Card key number refers to which key on the MIFARE card is used for access to the data on this AID/File. Typically this is 01, values can be 00 to 0D. Card key number of 0E is reserved for Free Read Access (no key needed).

Key Types:

- AES-128 (uses a 16 byte, 32 character key)
- 2KTDEA-DES (16 byte 3DES using MIFARE DESFire implementation). For single DES, repeat the 8-byte key.
- 2KTDEA-ISO and 3KTDEA (3DES using ISO-10116) are not available in firmware version 21.3 or 21.6

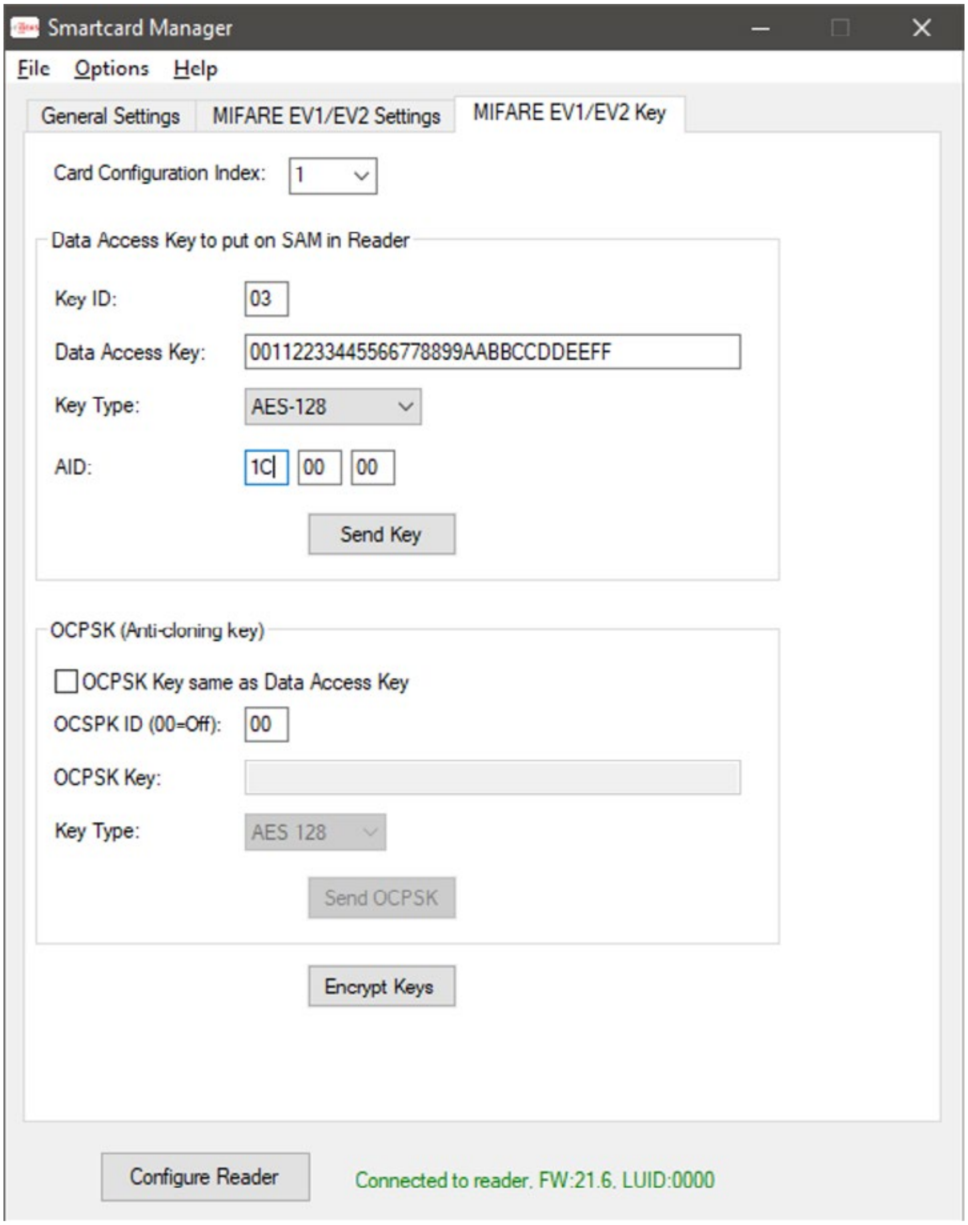
Signature Verification

This involves computing a signature from the data and comparing to a value on the card, using a key/process distinct from data encryption. This key used to make the signature is not stored on the card being read, and uses diversification, so a cloned card will fail the signature verification test. The Signature Verification process uses an additional key reference to the Originality and Cloning Protection System Key (OCPSK).

TIMING NOTE: Signature Verification requires additional data to be read and an additional encryption step. On a standard LEAF Cc card for instance, it nearly doubles the read and response time to about 1.5 seconds.

6. MIFARE® EV1/EV2 Key

Unless the file data is Free Access, a key will be needed to access the data. The key is stored on the NXP AV2 SAM (the removable SIM card). This key is kept separate in the reader from file configuration and other settings. It is not changed if the reader is set to defaults or boot loaded with new firmware. The keys can be programmed onto an AV2 SAM card on one reader, and then moved to another reader for use there. (AV2 SAM cards are only recognized at power-on, so the readers will need to be unplugged when moving the cards).



Card Configuration Index: 1

Data Access Key to put on SAM in Reader

Key ID: 03

Data Access Key: 00112233445566778899AABBCCDDEEFF

Key Type: AES-128

AID: 1C 00 00

OCPSK (Anti-cloning key)

□ OCPSK Key same as Data Access Key

OCSPK ID (00=Off): 00

OCPSK Key:

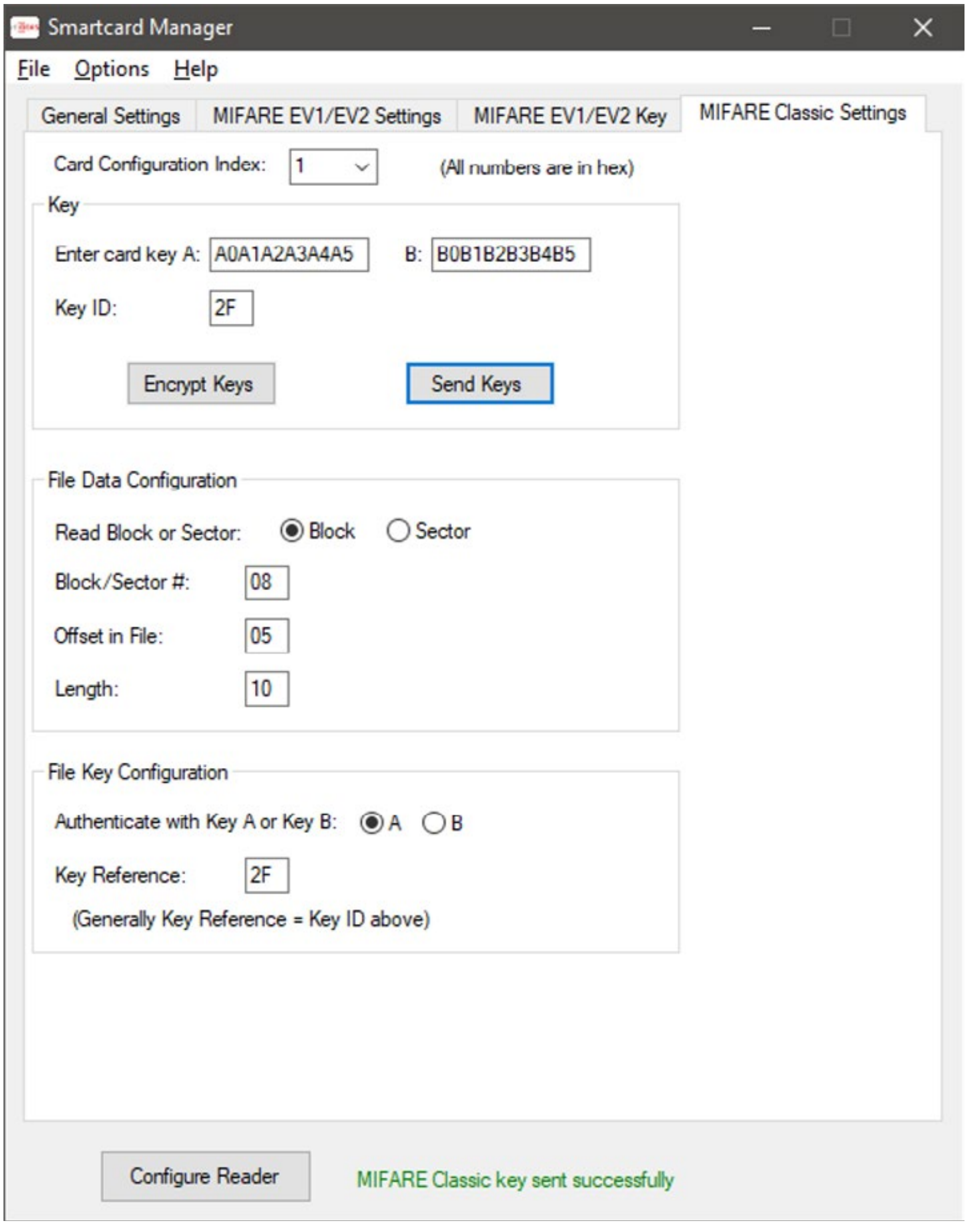
Key Type: AES 128

Connected to reader. FW:21.6. LUID:0000

For MIFARE DESFire® EV1/EV2, there are two places a key can be used, so there are two sections on this tab. First is Data Access. The AV2 SAM needs the AID stored with the key, so that information is duplicated from the EV1/EV2 Settings tab. The second section is for OCPSK, which can use the same key value as above if desired. AID is not needed for the OCPSK. Each section has its own Send button.

7. MIFARE Classic® Settings Tab

The MIFARE Classic card is simpler than the MIFARE® DESFire® EV1/EV2. Memory is also arranged differently, with sectors composed of blocks. Typically a sector has four blocks: three data blocks, and the last block has key and access information. They count from 0, so block 4 is the first data block of sector 1. Each block has 16 bytes, and each sector has 48 bytes of data.



Card Configuration Index: 1 (All numbers are in hex)

Key

Enter card key A: A0A1A2A3A4A5 B: B0B1B2B3B4B5

Key ID: 2F

File Data Configuration

Read Block or Sector: ● Block ○ Sector

Block/Sector #: 08

Offset in File: 05

Length: 10

File Key Configuration

Authenticate with Key A or Key B: ● A ○ B

Key Reference: 2F

(Generally Key Reference = Key ID above)

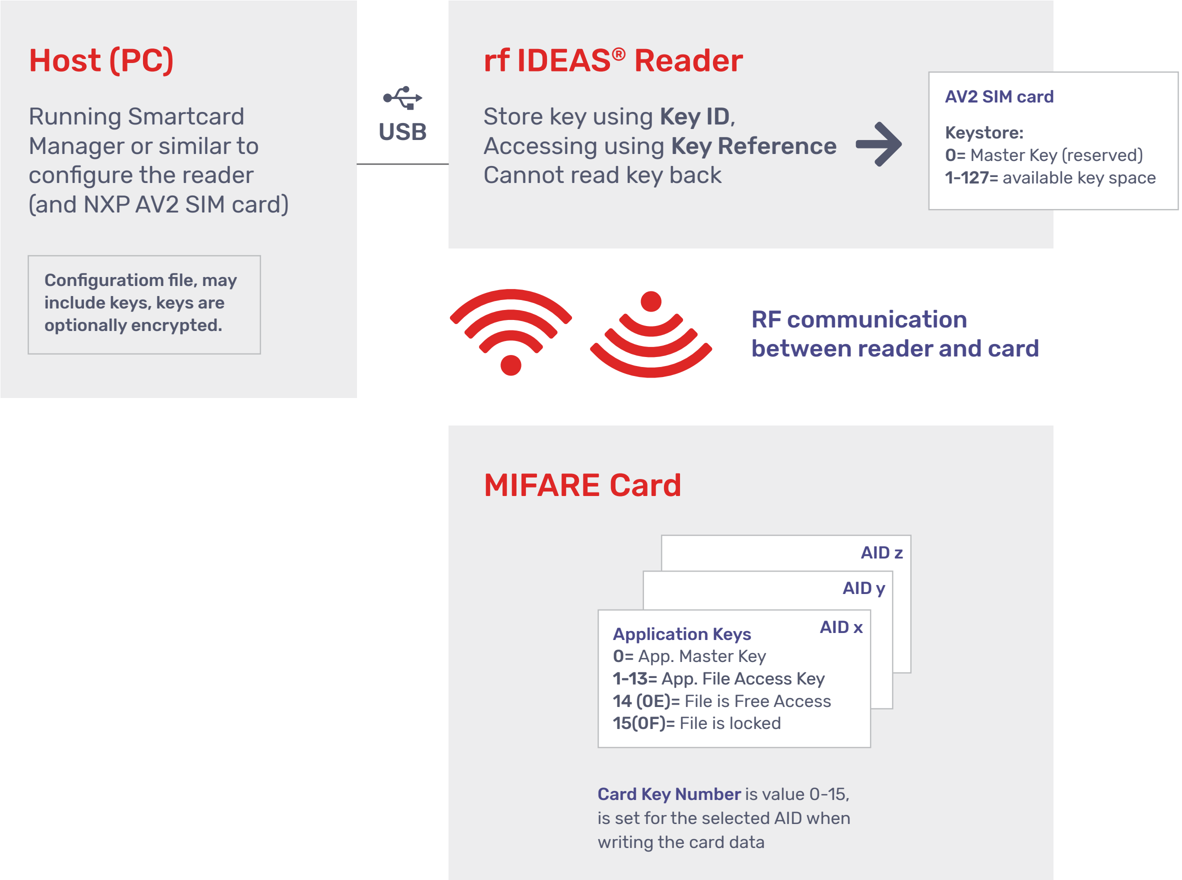
MIFARE Classic key sent successfully

There are two keys, each 6 bytes long. Typically Key A is used, but Key B is also possible. The two keys fit into one entry in the SAM AV2. Key ID and Key Reference values are the same as in MIFARE DESFire EV1/EV2. Note that the Configure Reader button at the bottom of the tab will not send the keys to the reader, the Send Keys button is used for that.

Note: The reader firmware has been extended for MIFARE Classic® to be able to keystroke up to 48 bytes of data (a typical sector). The SDK (API) interface, however, still has a maximum of 32 bytes. This is only noticeable if the configured length is more than 32 (hexadecimal 20), and the pcProxConfig utility (or similar application using our DLL) is used to retrieve data. The first 32 bytes are returned, and it reports a maximum of 255 bits of data.

8. MIFARE® Key Storage overview

The Key ID used when storing a key must be the same value that later will be used as the Key Reference when reading the data. They have a valid range of 1 to 127 (01 to 7F). The Card Key Number is an index to the key stored on the card, and that is a value 0 to 13. Card key number 14 (0E) is reserved for Free Access, and card key number 15 (0F) is No Access. See the following figure for specifics on keys, using the MIFARE DESFire® EV1/EV2 card as an example as it is the most complicated. The same general structure is also used in LEGIC® systems.



Host (PC)

Running Smartcard Manager or similar to configure the reader (and NXP AV2 SIM card)

Configuratiom file, may include keys, keys are optionally encrypted.

USB

rf IDEAS® Reader

Store key using **Key ID**,
Accessing using **Key Reference**
Cannot read key back

AV2 SIM card

Keystore:
0= Master Key (reserved)
1-127= available key space

RF communication between reader and card

MIFARE Card

AID z

AID y

AID x

Application Keys
0= App. Master Key
1-13= App. File Access Key
14 (0E)= File is Free Access
15(0F)= File is locked

Card Key Number is value 0-15, is set for the selected AID when writing the card data rf IDEAS

www.rfIDEAS.com

(847) 870-1723 | Toll-free: +1 (866) 439-4884 | sales@rfIDEAS.com

Trust begins here.™